ХАРЬКОВСКИЙ НАЦИОНАЛЬНЫЙ ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ

ЛЕКЦИЯ 2

Шифрование данных. Алгоритмы с секретным ключом. Алгоритмы с открытым ключом.

доцент кафедры информационных систем

к.т.н., с.н.с. Евсеев Сергей Петрович

ОСНОВНЫЕ ПОНЯТИЯ

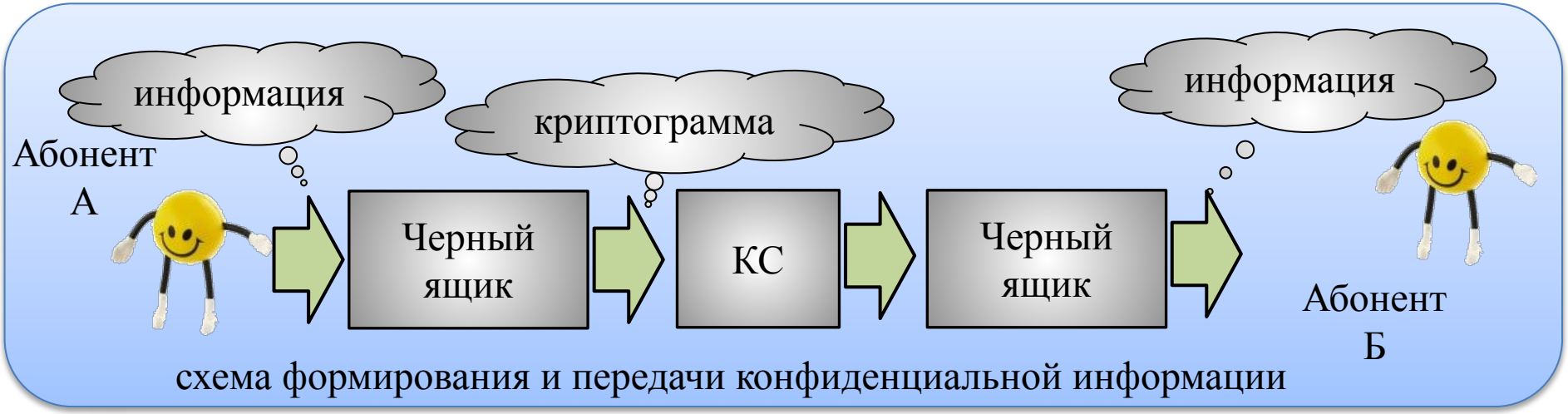


схема формирования и передачи конфиденциальной информации

Сообщение – исходный текст, представленный в цифровом виде.

Криптограмма – сообщение с искаженным логическим смыслом.

Шифрование данных – процесс преобразования открытых данных в зашифрованные данные при помощи шифра.

Шифр – множество обратимых преобразований множества сообщений во множество возможных криптограмм, по определенным правилам с применением ключей.

Ключ – конкретное секретное состояние некоторого параметра, обеспечивающее выбор одного преобразования из совокупности возможных для используемого метода шифрования.

.

ПРОСТЕЙШИЕ ШИФРЫ

ПЕРЕСТАНОВОЧНЫЙ ШИФР С КЛЮЧЕВЫМ СЛОВОМ

Буквы открытого текста записываются в клетки прямоугольной таблицы по ее строчкам.
Буквы ключевого слова пишутся над столбцами и указывают порядок этих столбцов (по возрастанию номеров букв в алфавите).
Чтобы получить зашифрованный текст, надо выписывать буквы по столбцам с учетом их алфавитного порядка.

Открытый текст: защита информации

Ключ: шифр

Криптограмма: аафа_иири_щ_оц_зтнми

ш	и	ф	р
4	1	3	2
з	а	щ	и
т	а		и
н	ф	о	р
м	а	ц	и
и			

МАТРИЧНАЯ ПЕРЕСТАНОВКА

Матричная перестановка представляет собой усложненную перестановку. Для этого открытый текст записывается в матрицу по определенному ключу $k_1=\{1, 2, \ldots, n\}$, который зависит от длины текста. Криптограмма получается при считывании из этой матрицы по ключу $k_2=\{1, 2, \ldots, m\}$. Размерность матрицы равна $n \times m$.

Открытый текст: "ШИФРОВАНИЕ_ПЕРЕСТАНОВКОЙ".

Ключи: k_1 5-3-1-2-4-6; k_2 4-2-3-1.

- запись по строкам в соответствии с ключом k_1
- чтение по столбцам в соответствии с ключом k_2

Криптограмма: "ПСНОРЙЕРВАИК_ЕАНФОИЕОТШВ".

1	и	е	_	п
2	е	р	е	с
3	о	в	а	н
4	т	а	н	о
5	ш	и	ф	р
6	в	к	о	й
$к_1/к_2$	1	2	3	4

ШИФР ПРОСТОЙ ЗАМЕНЫ

В процессе шифрования осуществляется преобразование открытого текста м длины l таким образом, что каждый символ заменяется на некоторый другой символ. При этом одинаковым символам в открытом тексте соответствуют одинаковые символы криптотекста, а разным символам – разные. Ключом является таблица в которой устанавливается правило замены символов, т.е. каждому символу a алфавита A, (a є A) ставится в соответствие символ b ≠ a из этого же алфавита A.

	0	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
$A_{рус}$	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ы	ъ	ь	э	ю	я
К	й	ц	у	к	е	н	г	ш	щ	з	х	ъ	ф	ы	в	а	п	р	о	л	д	ж	э	я	ч	с	м	и	т	ь	б	ю

Открытый текст: защита_информации
Криптограмма: шйсщой_щыдвпйэщщ

ШИФР ЦЕЗАРЯ

	0	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
$A_{рус}$	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ы	ъ	ь	э	ю	я
К	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ы	ъ	ь

Открытый текст: защита_информации
Криптограмма: дэцепэ_екслнйэуее

АФИННАЯ КРИПТОСИСТЕМА

Обобщением системы Цезаря является аффинная криптосистема. Она определяется двум числами ***a*** и ***b***, где **0** ≤***a***, ***b*** ≤*n-1. Где* ***n*** **–** мощность алфавита *A. Числа* ***a*** *и* ***n*** *должны быть взаимно просты, НОД(a,n) = 1.*

ШИФРОВАНИЕ

$$A_{a,b}(j) = (a*j+b)(\mathrm{mod}\ n)$$

РАСШИФРОВАНИЕ

$$A^{-1}_{a,b}(j) = (j-b)*a^{-1}(\mathrm{mod}\ n)$$

АЛГОРИТМ НАХОЖДЕНИЯ ВЗАИМНООБРАТНОГО ЧИСЛА

Исходные данные: $НОД(a,n) = 1$, $a \times a^{-1} \equiv 1 \mathrm{mod} n \Leftrightarrow a \equiv a^{-1} \mathrm{mod} n$

Правила вычислений:

1. Значения *x* и *y* берутся из предыдущей строки, значение *q* – из строки вычислений
2. Вычисления проводятся до тех пор пока значение в ячейке y_3 не будет равно 1, тогда в ячейке y_2 искомое a^{-1}. Если значение в ячейке отрицательное, то $a^{-1} = n - y_2$

q	x_1	x_2	x_3	y_1	y_2	y_3
	y_1	y_2	y_3	$x_1 - q\,y_1$	$x_2 - q\,y_2$	$x_3 - q\,y_3$
–	*1*	*0*	*n*	*0*	*1*	*a*

ШИФР ВИЖЕНЕРА И ЕГО МОДИФИКАЦИИ

А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А
В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б
Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В
Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г
Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д
Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е
З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж
И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З
Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И
К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й
Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К
М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л
Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М
О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н
П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О
Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П
С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	И	К	Л	М	Н	О	П	Р
Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	И	К	Л	М	Н	О	П	Р	С
У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т
Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У
Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф
Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х
Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц
Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч
Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш
Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ
Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ
Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы
Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь
Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э
Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю

По горизонтали – символы ключа.

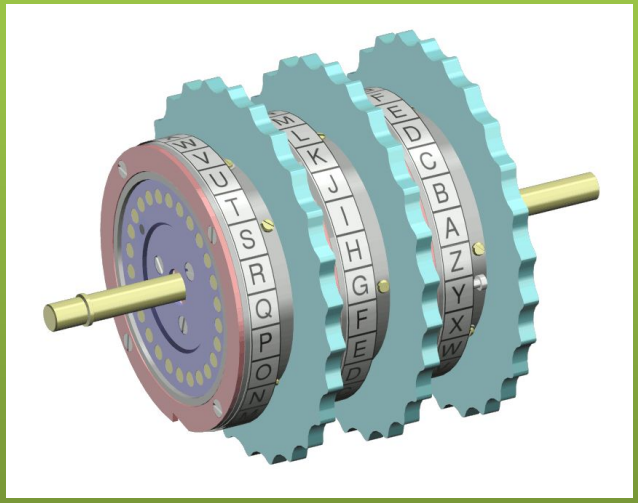
По вертикали – символы открытого текста

В шифре с автоключом с использованием открытого текста после использования символов ключа используются символы открытого текста в качестве символов ключа

ПОЛИАЛФАВИТНАЯ ЗАМЕНА

	0	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
$A_{рус}$	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ы	ъ	ь	э	ю	я
$f_0(x)$	й	ц	у	к	е	н	г	ш	щ	з	х	ъ	ф	ы	в	а	п	р	о	л	д	ж	э	я	ч	с	м	и	т	ь	б	ю
$f_1(x)$	м	и	т	ь	б	ю	й	ц	у	к	е	н	г	ш	щ	з	х	ъ	ф	ы	в	а	п	р	о	л	д	ж	э	я	ч	с
$f_2(x)$	р	о	л	д	ж	э	я	ч	с	м	и	т	ь	б	ю	й	ц	у	к	е	н	г	ш	щ	з	х	ъ	ф	ы	в	а	п
$f_3(x)$	ш	щ	з	х	ъ	ф	ы	в	а	п	р	о	л	д	м	и	т	ь	б	ю	й	ц	у	к	е	н	г	ж	э	я	ч	с

Данный класс шифров объединил в себе два вида математических преобразований перестановки f и подстановки g. С помощью операции перестановки формируется ключевая матрица подстановки, состоящая из нескольких различных функций f_i . С помощью подстановки g производится шифрование открытого текста. Формирование ключа. Выбираются случайные перестановки базового алфавита.



ЧАСТОТНЫЙ КРИПТОАНАЛИЗ

Криптоанализ – область криптологии, в которой рассматриваются вопросы взлома шифров с целью восстановления информации в открытом виде или фальсификации шифрованной информации, которая впоследствии должна быть принята как подлинная.

Распределение букв очень сильно зависит от типа теста: проза, разговорный язык, технический язык и т.п.

Распределение букв в криптотексте сравнивается с распределением букв в алфавите исходного сообщения. Буквы с наибольшей частотой в криптотексте заменяются на букву с наибольшей частотой из алфавита. Вероятность успешного вскрытия повышается с увеличением длины криптотекста.

ЧАСТОТА ПОЯВЛЕНИЯ СИМВОЛОВ В РУССКОМ ЯЗЫКЕ

Бука	Частота	Бука	Частота	Бука	Частота
а	0,062	л			
б	0,014	м			
в	0,038	н			
г	0,013	о			
д	0,025	п			
е	0,072	р			
ж	0,007	с			
з	0,016	т			
и	0,062	у			
к	0,010	ф			

УСЛОВНАЯ ЧАСТОТА ПОЯВЛЕНИЯ СИМВОЛВ В КРИПТОГРАММЕ

Бука	Частота	Бука	Частота	Бука	Частота
а	0,043	л	0,001	х	0,009
б	0,039	м	0,001	ц	0,004
в	0,054	н	0,035	ч	0,012
г	0,012	о	0,090	ш	0,006
д	0,075	п	0,023	щ	0,003
е	0,008	р	0,040	ы	0,016
ж	0,007	с	0,045	ь, ъ	0,014
з	0,011	т	0,053	э	0,003
и	0,009	у	0,021	ю	0,006
к	0,001	ф	0,002	я	0,018

ОСНОВНЫЕ ТЕОРЕМЫ ШИФРОВАНИЯ

Теорема Эйлера

Пусть $m>1$, $gsd(a,m)=1$, j (m) – функция Эйлера.
Тогда: $a^{j(m)} \equiv 1(mod\ m)$.

Теорема Ферма

Если p – простое число, и a не делится на p, то $a^{p-1} \equiv 1(mod p)$.
Другими словами, a^{p-1} при делении на целое на p даёт в остатке 1.

Китайская теорема об остатках

Пусть n_i, $1 \le i \le k$, взаимно простые числа
и пусть a_i целые числа. Тогда существует такое число x,
что имеет место:

$$x \equiv a_1 \bmod n_1,$$
$$x \equiv a_2 \bmod n_2,$$
$$\dots$$
$$x \equiv a_k \bmod n_k .$$

Теорема утверждает, что можно восстановить целое число по множеству его остатков от деления на числа из некоторого набора попарно взаимнопростых чисел.

КЛАССИФИКАЦИЯ АЛГОРИТМОВ ШИФРОВАНИЯ

Безключевые

- Хэш-функции
- Генераторы случайных чисел

Одноключевые

- Хэш-функции
- Генераторы псевдослучайных чисел
- Алгоритмы симметричного шифрования

Двухключевые

- Алгоритмы шифрования с открытым ключом
- Алгоритмы цифровой подписи
- Алгоритмы аутентификации

Секретной системой называется совокупность множеств открытых текстов и криптограмм, множеств прямых и обратных отображений, множества ключей.

Если $K \neq K^*$, то система *асимметрична*. Напротив, если $K = K^*$ – *симметрична*.

МОДЕЛИ СЕКРЕТНЫХ СИСТЕМ:
совершенная стойкость (Perfect Secrecy);
доказуемая стойкость ("Provable" Security);
временная стойкость (Practical Security).

МОДЕЛИ СЕКРЕТНЫХ СИСТЕМ

Временная стойкость (Practical Security). Криптограмма формируется путем многократного выполнения одинаковых групп преобразований, в результате обеспечивается высокий уровень перемешивания и рассеивания информационных блоков данных. *Преимущество* - высокая скорость преобразования и простота реализации. Существенным *недостатком* - отсутствие строгого математического обоснования криптографической стойкости. (Относятся все алгоритмы симметричной криптографии).

Доказуемая стойкость ("Provable" Security).
Задача взлома ключевых данных сводится к решению известной математической задачи. Сложность взлома которых сведена к решению одной из теоретико-сложностных задач. *Преимущество* – обеспечивается доказуемая (с математической точки) криптостойкость. Существенным *недостатком* – низкая скорость шифрования, на 3-5 порядков ниже, чем у симметричных криптоалгоритмов. (Относятся все алгоритмы несимметричной криптографии).

Совершенная стойкость (Perfect Secrecy).
Шифр простой замены (шифр Вернама) обеспечивает совершенную стойкость. Необходимыми условиями построения совершенной секретной системы является большой объем ключевых данных, по крайней мере, бóльший мощности множества открытых текстов и равновероятное формирование ключевых данных. Модель совершенной стойкости (безусловной безопасности) введена в предположении о неограниченных вычислительных ресурсах злоумышленника и на практике используется крайне редко.

ОСНОВНЫЕ ПОКАЗАТЕЛИ СЕКРЕТНЫХ СИСТЕМ

Криптографическая стойкость (количество секретности), которую оценивают как сложность решения задачи криптоанализа наилучшим известным методом.

Объем ключевых данных. Для симметричных систем ключ общий для всех пользователей системы и его нужно передавать по закрытым каналам связи. Если система несимметричная, то один из ключей можно сделать общедоступным и передавать его по открытым каналам связи.

Сложность выполнения прямого и обратного криптографического преобразования. Операции должны быть по возможности простыми и легко реализуемыми на практике.

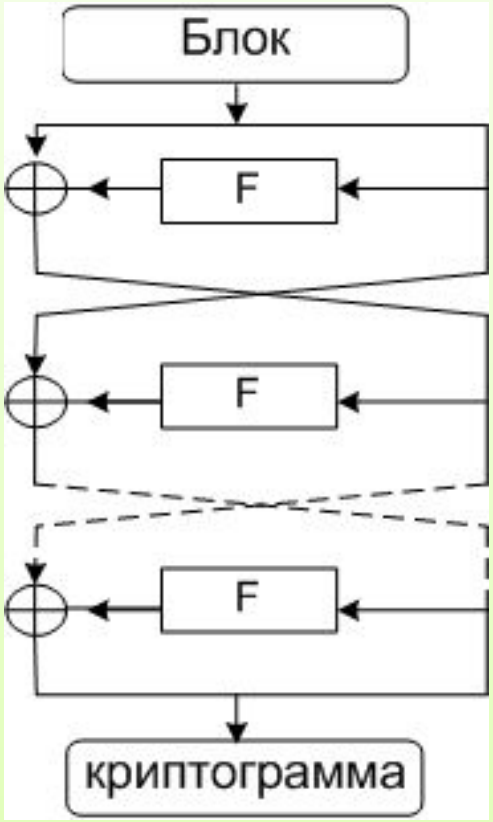
Разрастание числа ошибок. Ошибки разрастаются в результате операции расшифрования, вызывая значительную потерю информации и часто требуя повторной передачи криптограммы. Естественно, желательно минимизировать это возрастание числа ошибок.

Увеличение объема сообщения. В некоторых типах секретных систем объем сообщения увеличивается в результате операции шифрования. Этот нежелательный эффект нужно минимизировать.

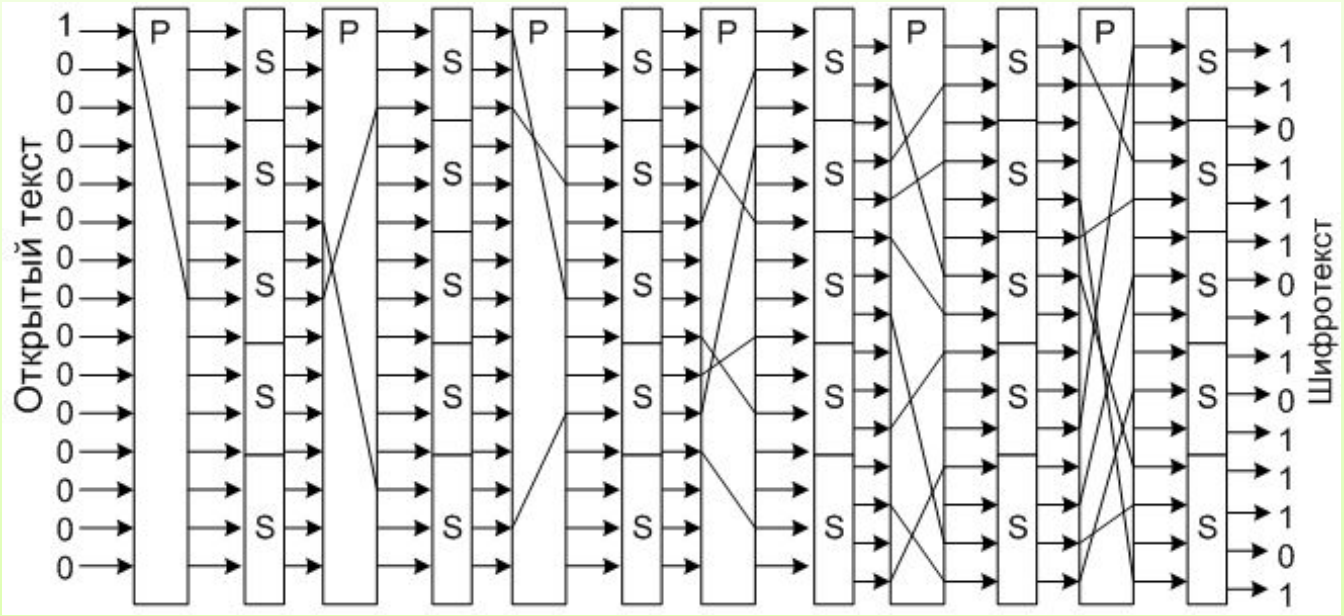
СИММЕТРИЧНЫЕ КРИПТОСИСТЕМЫ

Основное различие между блочными и поточными методами состоит в том, что блочные методы применяют одно постоянное преобразование к фиксированным блокам данных открытого текста; поточные методы применяют изменяющиеся во времени преобразования к отдельным символам открытого текста.

НЕЛИНЕЙНЫЕ УЗЛЫ ЗАМЕН СИММЕТРИЧНЫХ КРИПТОАЛГОРИТМОВ. БЛОЧНЫЕ АЛГОРИТМЫ



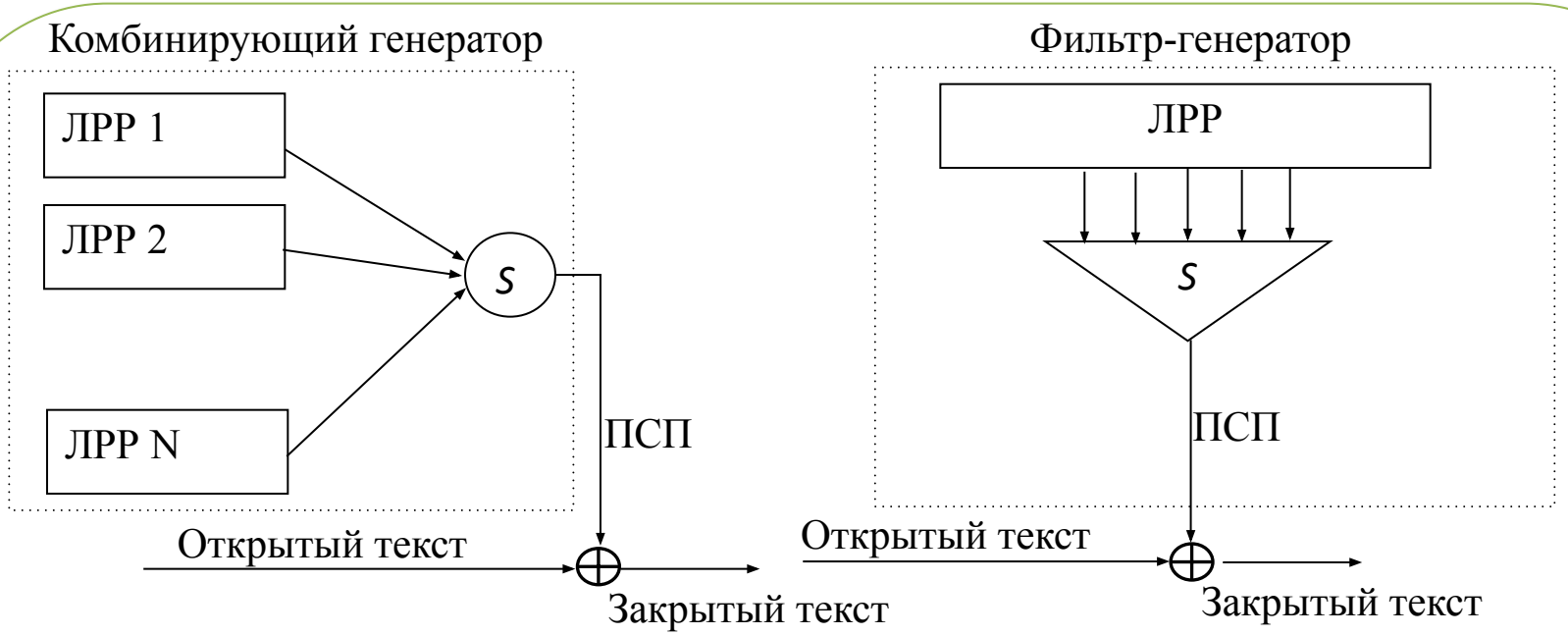
информация разбивается на n блоков и на каждом цикле подвергается преобразованию при помощи криптографической функции F



SPN-цепи простейших криптопреобразователей (криптопримитивов - P и S-блоки) в которых шифрующая функция работает сразу со всем блоком.

Стойкость нелинейных узлов замен, осуществляющих необратимые/труднообратимые нелинейные преобразования, определяют эффективность симметричных криптографических средств защиты информации.

НЕЛИНЕЙНЫЕ УЗЛЫ ЗАМЕН СИММЕТРИЧНЫХ КРИПТОАЛГОРИТМОВ. ПОТОЧНЫЕ АЛГОРИТМЫ



Строятся посредством комбинирующих генераторов, в которых используется нескольких параллельно работающих линейных рекуррентных регистров, вырабатывающих ***гамму***, и используется метод преобразования информации с неравномерным движением регистров или фильтр-генераторов с одним линейным рекуррентным регистром и равномерным движением регистров

ПОКАЗАТЕЛИ ЭФФЕКТИВНОСТИ КРИПТОГРАФИЧЕСКИХ БУЛЕВЫХ ФУНКЦИЙ (НЕЛИНЕЙНЫХ УЗЛОВ ЗАМЕН)

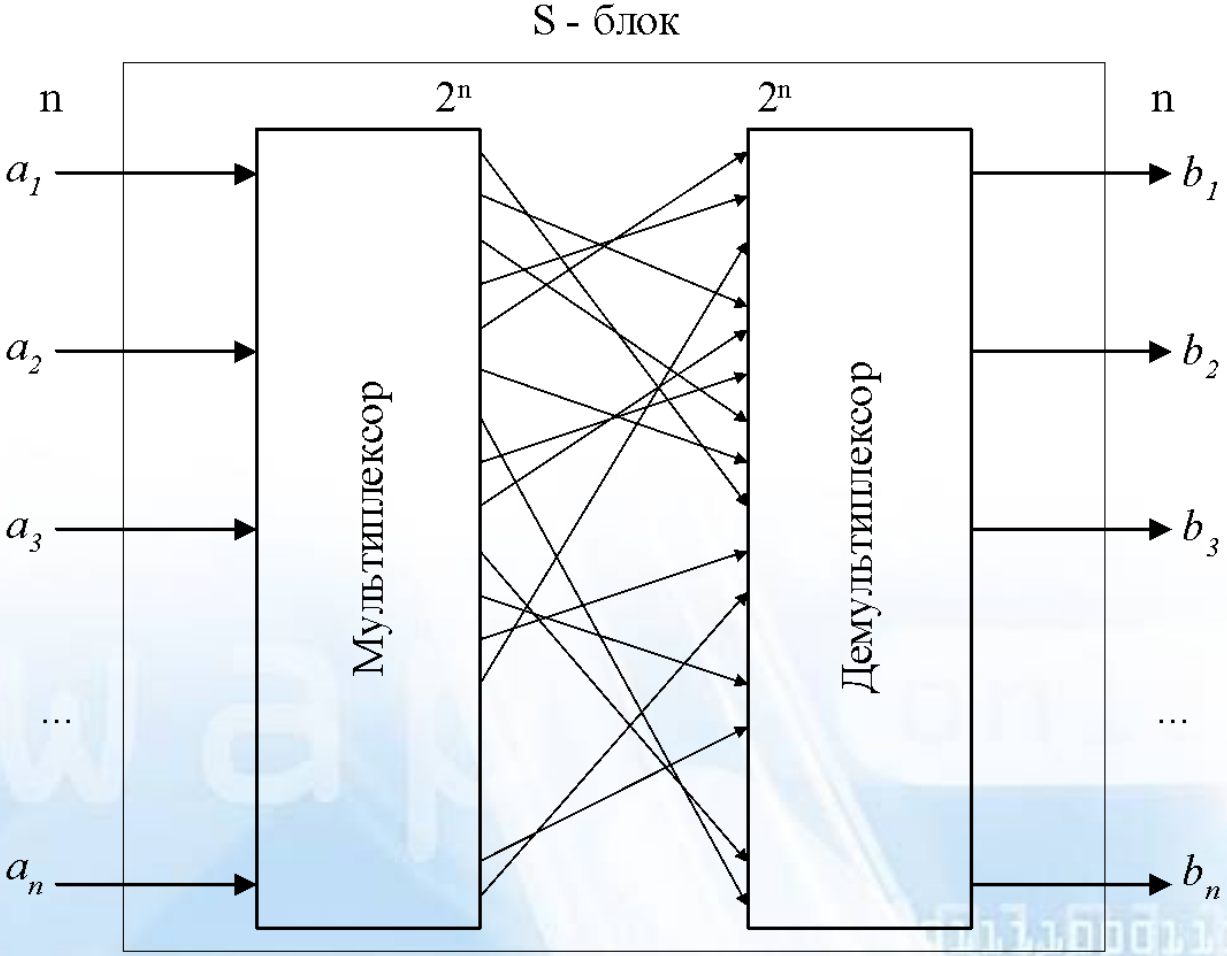


Схема преобразования данных в нелинейном узле замены

Основными показателями эффективности криптографических булевых функций (собственно и самого нелинейного узла замен) являются:

- сбалансированность,
- нелинейность,
- алгебраическая степень,
- значение функции автокорреляции,
- степень корреляционного иммунитета,
- степень критерия распространения.

ПОКАЗАТЕЛИ ЭФФЕКТИВНОСТИ КРИПТОГРАФИЧЕСКИХ БУЛЕВЫХ ФУНКЦИЙ (НЕЛИНЕЙНЫХ УЗЛОВ ЗАМЕН)

Сбалансированность Сб – равенство числа нулей и единиц в выходной последовательности:

$$| \{x \mid f(x) = 0\} | = | \{x \mid f(x) = 1\} | = 2^{n-1}. \quad (1)$$

Нелинейность N_S преобразования – **минимальное расстояние Хэмминга между выходной последовательностью *S* и всеми последовательностями аффинных функций *ϕ*:**

$$N_S = min\ \{d(S,\phi)\}. \quad (2)$$

Алгебраическая степень – степень самого длинного слагаемого функции, представленной в алгебраической нормальной форме:

$$f(x_1,\ldots,x_n) = a_0 \oplus \bigoplus_{i=1}^{n} a_i x_i \oplus \bigoplus_{1\le i<j\le 1} a_{ij} x_i x_j \oplus \ldots \oplus a_{12\ldots n} x_1 x_2 \cdots x_n \quad (3)$$

***Значение функции автокорреляции AC* – максимальное по модулю значение корреляции ко всем входным векторам**

$$AC(f) = \max_{s\neq 0} \left| \sum_{ч} \hat{f}\ (x)\hat{f}\ (x \oplus s) \right| = \max_{s\neq 0} \left| \hat{r}\ (s) \right| \quad (4)$$

Корреляционный иммунитет КИ(*f*) порядка *k* – статистическая независимость выходной последовательности *y* ∈ *Y* от любого подмножества из *k* входных координат:

$$\forall \{x_1, \ldots, x_k\}\ P(y \in Y / \{x_1, \ldots, x_k\} \in X) = P(y \in Y). \quad (5)$$

В терминах преобразования Уолша: $КИ(f) = k$, если $F(\omega) = 0,\ \forall \omega \in V_n,\ 1 \le W(\omega) \le k$, где

$$F(\omega) = 2^{-n}, \quad (6)$$

$\langle \omega, x \rangle$ – скалярное произведение $(w_1x_1 \oplus \ldots \oplus w_nx_n)$.

Критерий распространения КР относительно вектора *α* – сбалансированность функции

$$f(x) \oplus f(x \oplus \alpha),\ x \in V_n,\ x = (x_1, x_2, \ldots, x_n). \quad (7)$$

Строгий лавинный критерий – $КР\ \forall \alpha : 1 \le W(\alpha) \le k$.

ФУНКЦИОНАЛ ЭФФЕКТИВНОСТИ НЕЛИНЕЙНЫХ УЗЛОВ ЗАМЕН

$S_{ПТ} = f(S_{НБФ}) = f(S_{СБ}, S_N, S_{DEG}, S_{CIPC}, S_{AC})$, где

- Сбалансированность функции $S_{СБ}$ – стойкость к статистическим атакам;
- Нелинейность функции – стойкость к корреляционным атакам

$$S_N = \max_{S_j}\{S_{N1}, ..., S_{Nr}\};$$

- Алгебраическая степень – стойкость к аналитическим атакам

$$S_{DEG}(f) = \max_{Sdeg(f_j)}\{S_{DEG}(f_1), ..., S_{DEG}(f_r)\};$$

- Степень корреляционного иммунитета/критерия распространения – стойкость к корреляционным атакам $S_{CIPC}(f) = \max_{SCIPS(f_j)}\{S_{CIPC}(f_1), ..., S_{CIPC}(f_r)\};$
- Значение автокорреляции – стойкость функций к классу аналитических атак

$$S_{AC}(f) = \max_{SAC(f_j)}\{S_{AC}(f_1), ..., S_{AC}(f_r)\};$$

БЕЗОПАСНОСТЬ ТРАДИЦИОННОЙ КРИПТОГРАФИИ

- Криптографический алгоритм должен быть достаточно сильным, чтобы передаваемое зашифрованное сообщение невозможно было расшифровать без ключа, используя только различные статистические закономерности зашифрованного сообщения или какие-либо другие способы его анализа.
- Безопасность передаваемого сообщения должна зависеть от секретности ключа, но не от секретности алгоритма.
- Алгоритм должен быть таким, чтобы нельзя было узнать ключ, даже зная достаточно много пар (зашифрованное сообщение, незашифрованное сообщение), полученных при шифровании с использованием данного ключа.

АЛГОРИТМ DES (DATA ENCRYPTION STANDARD).

DES (Data Encryption Standard). Алгоритм был разработан в 1977 году, в 1980 году был принят NIST (National Institute of Standards and Technolody США) в качестве стандарта (FIPS PUB 46).

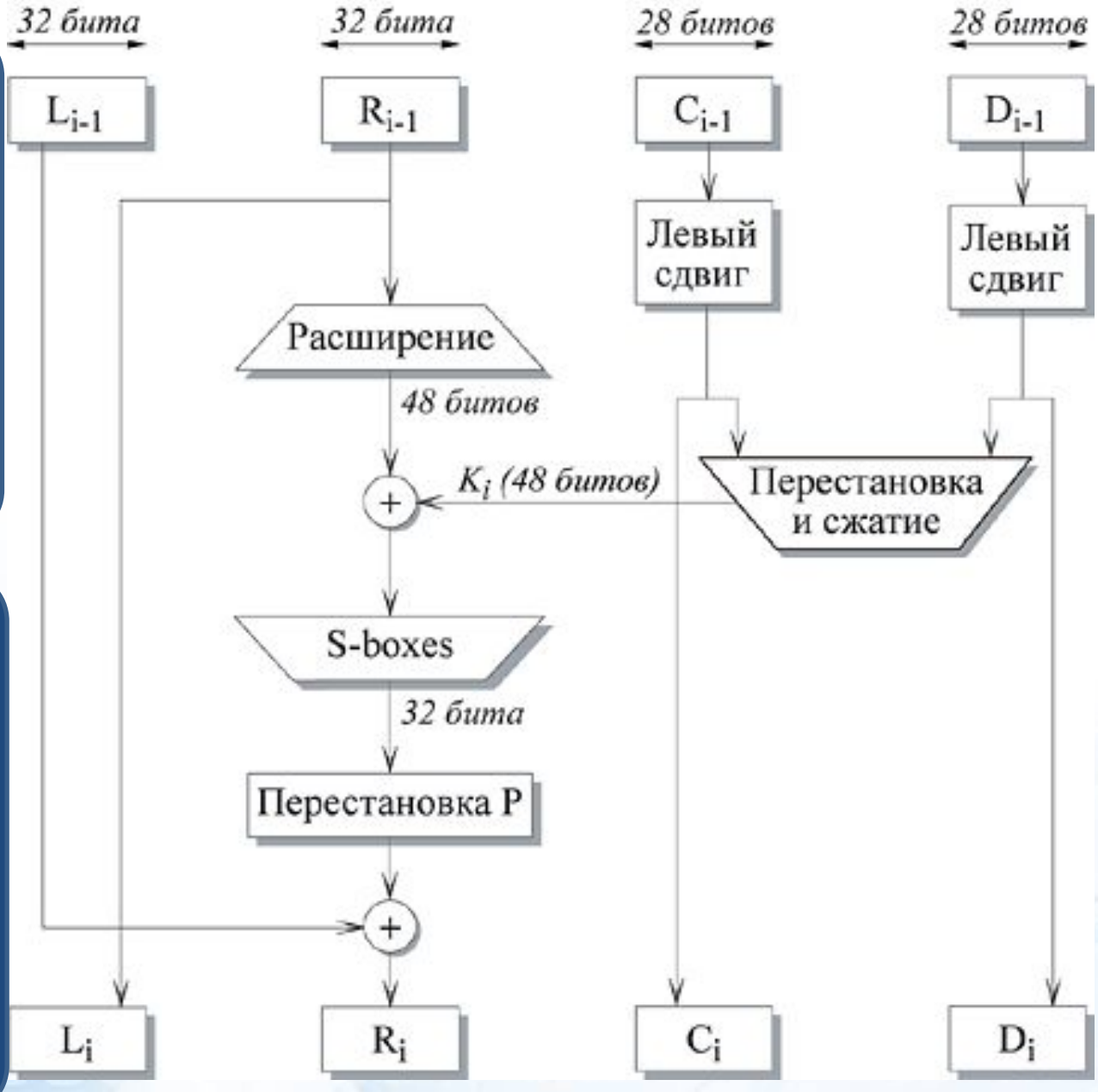
Начальная перестановка и ее инверсия определяются стандартной таблицей.
Если M - это произвольные 64 бита, то X = IP (M) - переставленные 64 бита.
Если применить обратную функцию перестановки $Y = IP^{-1}(X) = IP^{-1}(IP(M))$, то получится первоначальная последовательность битов.

Общая схема DES

АЛГОРИТМ DES (DATA ENCRYPTION STANDARD).

64-битный входной блок проходит через 16 раундов, при этом на каждой итерации получается промежуточное 64-битное значение. Левая и правая части каждого промежуточного значения трактуются как отдельные 32-битные значения, обозначенные L и R.

Подстановка состоит из восьми S-boxes , каждый из которых на входе получает 6 бит, а на выходе создает 4 бита. Эти преобразования определяются специальными таблицами. Первый и последний биты входного значения S-box определяют номер строки в таблице, средние 4 бита определяют номер столбца.



I-ый раунд DES

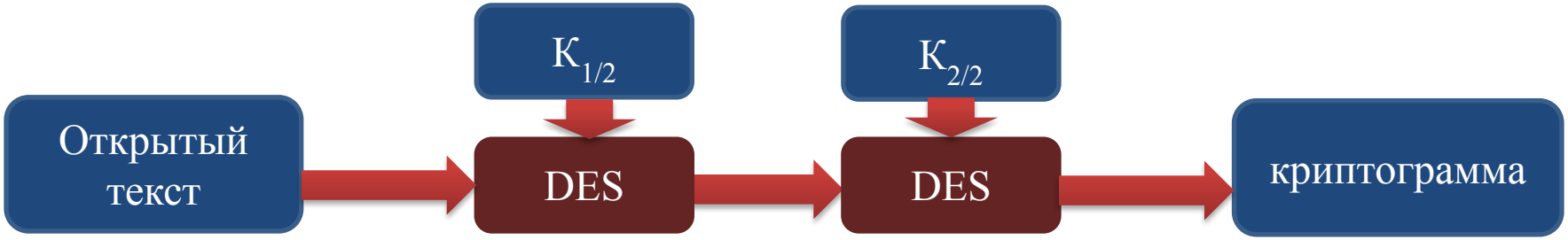
АЛГОРИТМ DES (DATA ENCRYPTION STANDARD). СОЗДАНИЕ КЛЮЧЕЙ

Ключ для отдельного раунда K_i состоит из 48 битов. Ключи K_i получаются по следующему алгоритму. Для 56-битного ключа, используемого на входе алгоритма, вначале выполняется перестановка в соответствии с таблицей Permuted Choice 1 (PC-1).

Полученный 56-битный ключ разделяется на две 28-битные части, обозначаемые как C_0 и D_0 соответственно.

На каждом раунде C_i и D_i независимо циклически сдвигаются влево на 1 или 2 бита, в зависимости от номера раунда. Полученные значения являются входом следующего раунда. Они также представляют собой вход в Permuted Choice 2 (PC-2), который создает 48-битное выходное значение, являющееся входом функции $F(R_{i-1}, K_i)$.

АЛГОРИТМ DOUBLE DES

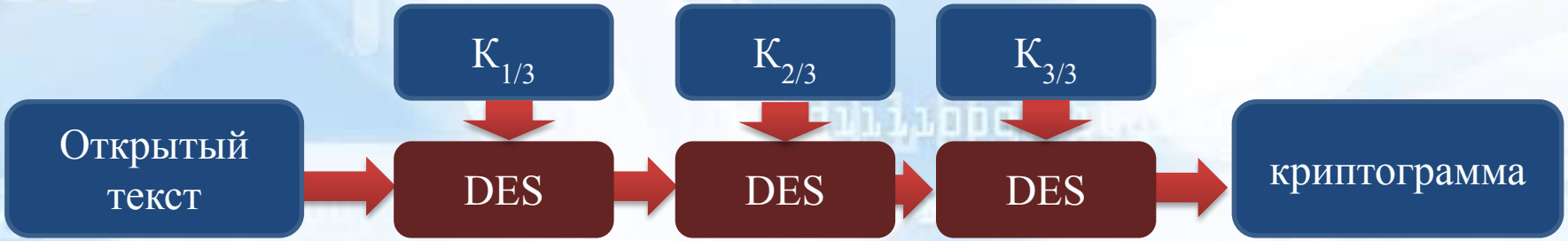


Double DES, представляющий собой двойное шифрование обычным DES'ом:

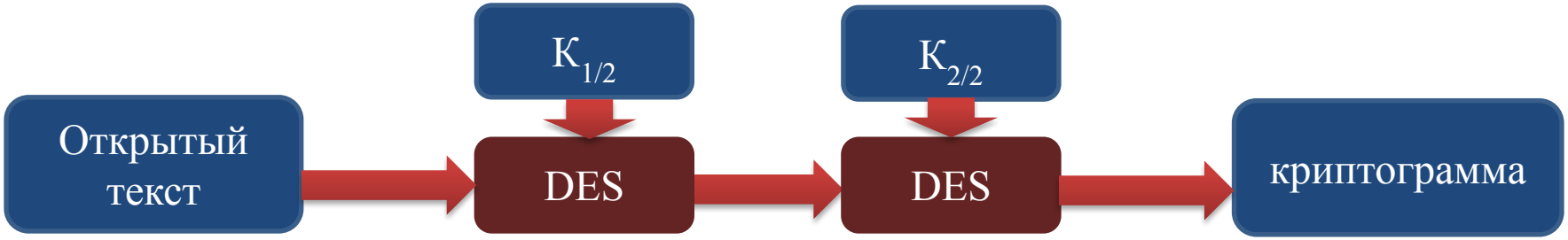
$$C = DES_{k2/2}(DES_{k1/2}(M)),$$

где $k_{1/2}$ и $k_{2/2}$ – половины двойного ключа алгоритма Double DES, каждая из которых представляет собой обычный 56-битный ключ DES.

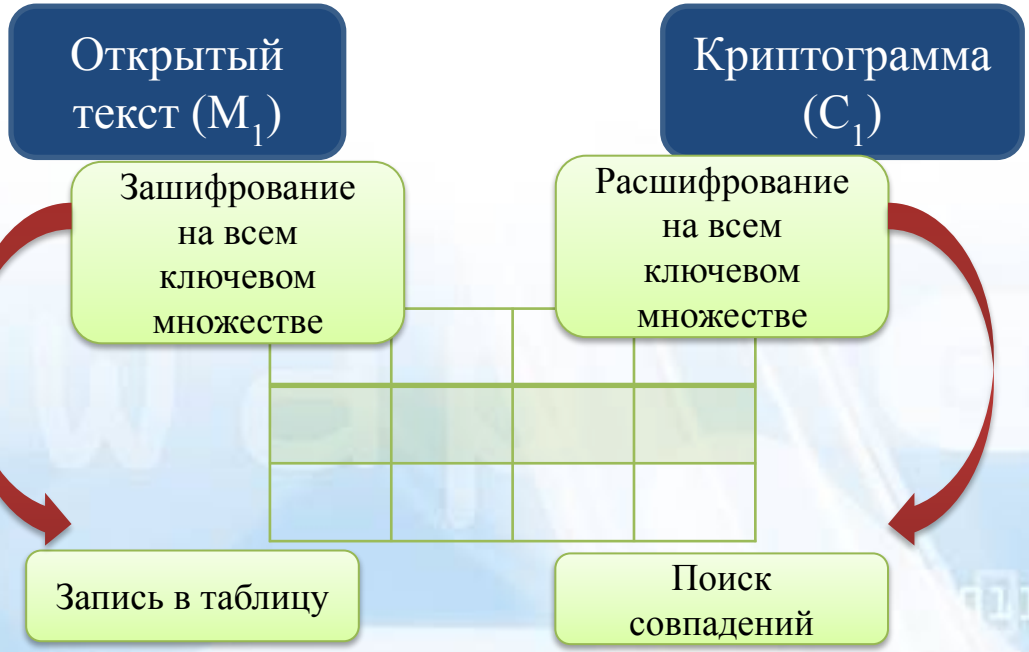
АЛГОРИТМ TRIPLE DES



АЛГОРИТМ DOUBLE DES



АТАКИ КЛАССА «ВСТРЕЧА ПОСЕРЕДИНЕ» (MEET-IN-THE-MIDDLE)



- Выполняется зашифрование $\mathbf{DES_{kx}(M1)}$ на всем ключевом множестве ($\mathbf{kx} = 0\ldots2^{56}\text{-}1$) с записью результатов в некоторую таблицу.
- Производится расшифрование $\mathbf{DES^{-1}_{ky}(C1)}$ также на всем ключевом множестве; результаты расшифрования сравниваются со всеми записями в таблице, сформированной на шаге 1.
- Если какой-либо результат, полученный на шаге 2, совпал с одним из результатов шага 1, то можно предположить, что нужный ключ найден, т.е. соответствующие совпадающему результату $\mathbf{kx = k_{1/2}}$, а $\mathbf{ky = k_{2/2}}$.

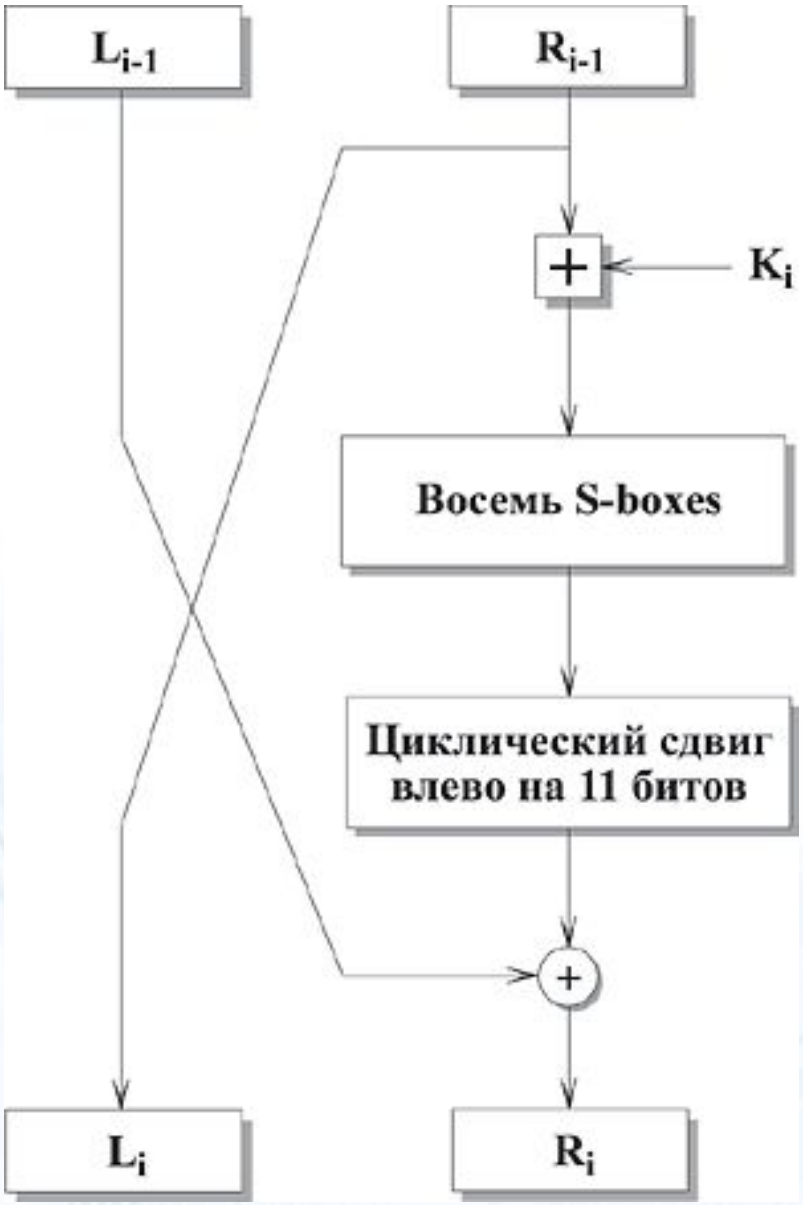
Сложность вычисления ключа Double DES всего в 2 раза выше, чем полный перебор ключей обычного DES

АЛГОРИТМ ГОСТ 28147

ГОСТ 28147 разработан в 1989 году, является блочным алгоритмом шифрования, длина блока равна 64 битам, длина ключа равна 256 битам, количество раундов равно 32. Алгоритм представляет собой классическую сеть Фейстеля.

Функция F проста. Сначала правая половина и i-ый подключ складываются по модулю 2^{32}. Затем результат разбивается на восемь 4-битовых значений, каждое из которых подается на вход S-box.

ГОСТ 28147 использует восемь различных S-boxes, каждый из которых имеет 4-битовый вход и 4-битовый выход. Выходы всех S-boxes объединяются в 32-битное слово, которое затем циклически сдвигается на 11 битов влево. Наконец, с помощью XOR результат объединяется с левой половиной, в результате чего получается новая правая половина.



I-ый раунд ГОСТ 28147

АЛГОРИТМ ГОСТ 28147. СОЗДАНИЕ КЛЮЧЕЙ

256-битный ключ разбивается на восемь 32-битных подключей. Алгоритм имеет 32 раунда, поэтому каждый подключ используется в четырех раундах по следующей схеме:

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

Порядковый номер числа будет являться входным значением S-box, а само число - выходным значением S-box.

1-ый S-box	4	10	9	2	13	8	0	14
	6	**11**	**1**	**12**	**7**	**15**	**5**	**3**
2-ой S-box	14	11	4	12	6	13	15	10
	2	**3**	**8**	**1**	**0**	**7**	**5**	**9**
3-ий S-box	5	8	1	13	10	3	4	2
	14	**15**	**12**	**7**	**6**	**0**	**9**	**11**
4-ый S-box	7	13	10	1	0	8	9	15
	14	**4**	**6**	**12**	**11**	**2**	**5**	**3**
5-ый S-box	6	12	7	1	5	15	13	8
	4	**10**	**9**	**14**	**0**	**3**	**11**	**2**
6-ой S-box	4	11	10	0	7	2	1	13
	3	**6**	**8**	**5**	**9**	**12**	**15**	**14**
7-ой S-box	13	11	4	1	3	15	5	9
	0	**10**	**14**	**7**	**6**	**8**	**2**	**12**
8-ой S-box	1	15	13	0	5	7	10	4
	9	**2**	**3**	**14**	**6**	**11**	**8**	**12**

ОСНОВНЫЕ РАЗЛИЧИЯ МЕЖДУ DES И ГОСТ 28147

- DES использует гораздо более сложную процедуру создания подключей, чем ГОСТ 28147. В ГОСТ эта процедура очень проста.
- В DES применяется 56-битный ключ, а в ГОСТ 28147 - 256-битный. При выборе сильных S-boxes ГОСТ 28147 считается очень стойким.
- У S-boxes DES 6-битовые входы и 4-битовые выходы, а у S-boxes ГОСТ 28147 4-битовые входы и выходы. В обоих алгоритмах используется по восемь S-boxes, но размер S-box ГОСТ 28147 существенно меньше размера S-box DES.
- В DES применяются нерегулярные перестановки P, в ГОСТ 28147 используется 11-битный циклический сдвиг влево. Перестановка DES увеличивает лавинный эффект. В ГОСТ 28147 изменение одного входного бита влияет на один S-box одного раунда, который затем влияет на два S-boxes следующего раунда, три S-boxes следующего и т.д. В ГОСТ 28147 требуется 8 раундов прежде, чем изменение одного входного бита повлияет на каждый бит результата; DES для этого нужно только 5 раундов.
- В DES 16 раундов, в ГОСТ 28147 - 32 раунда, что делает его более стойким к дифференциальному и линейному криптоанализу.

УСКОРЕНИЕ ГОСТ 28147

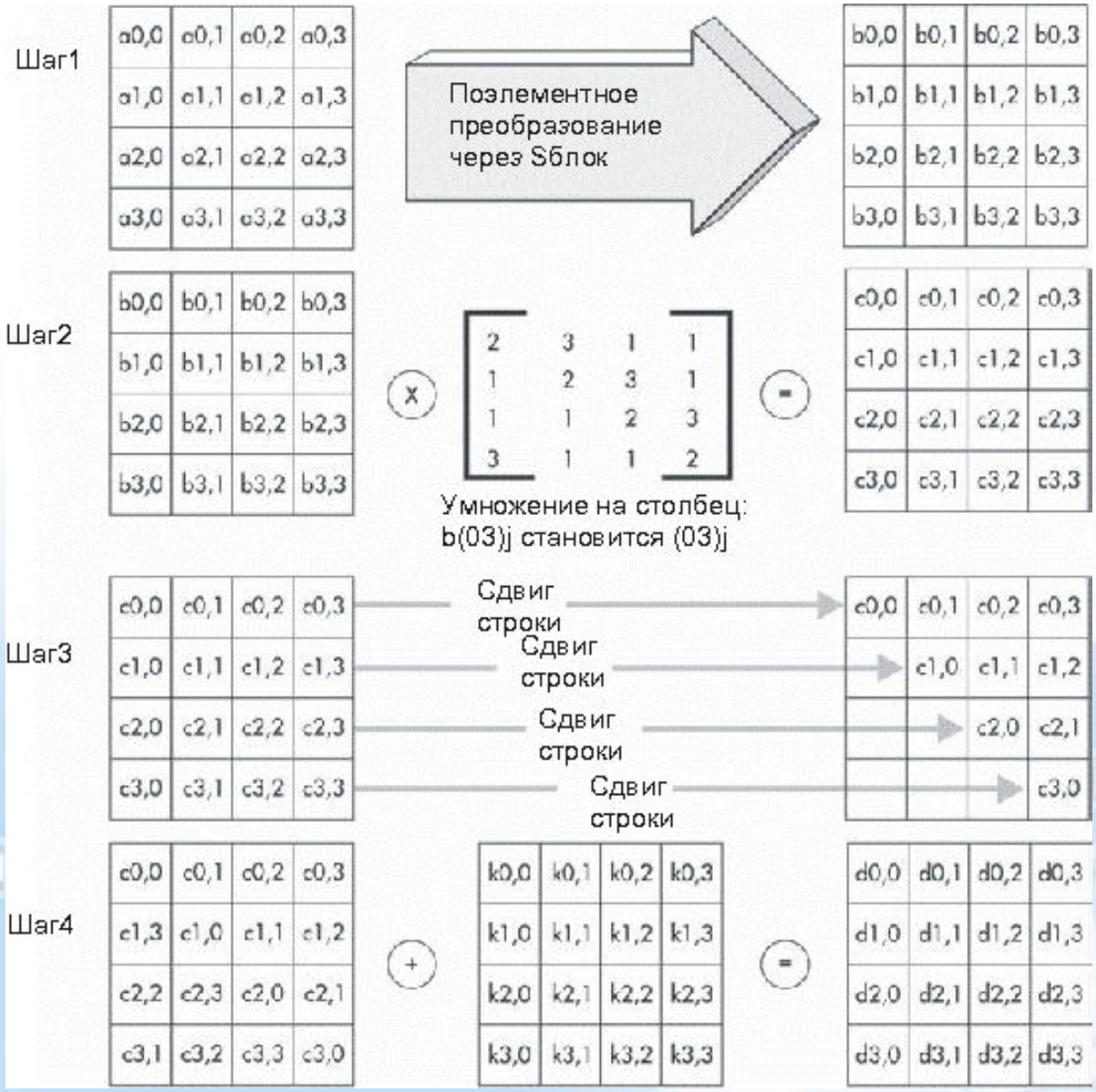
- применение SSE регистров и конвейерного выполнения операций для двух независимых вычислительных потоков позволяет достичь скорость обработки в районе 350 Мбайт/с. для одного процессорного ядра с частотой 3.6гГц.

- Старые методы реализации алгоритма, с использованием РОН не давали скорости большей 35 Мбайт/с.

- Теоретически, если реализовать алгоритм не на 128 битных XMM регистрах, а на 256 битных YMM регистрах, по скорость преобразования можно было поднять еще в два раза

- процессора Skylake выполняют команды использующие YMM регистры с той же скоростью что и команды с использованием XMM регистров. Соответственно, появилась возможность ускорить реализацию алгоритма преобразования по ГОСТ 28147-89 ровно в два раза, за счет увеличения количества одновременно обрабатываемых блоков данных с 8 до 16.

ДСТУ 7624-2015 Алгоритм симметричного блочного преобразования «Калина-256»



Общая структура - SPN, square-type, байт-ориентированный шифр. Структура алгоритма аналогична структуре Rijndael.

Используются циклы преобразования 2-х типов: с вводом ключа по модулю 2 и по модулю 2^{32}, что увеличивает нелинейность шифра, вводит дополнительные зависимости между результирующими значениями.

РЕЖИМЫ РАБОТЫ БЛОЧНЫХ АЛГОРИТМОВ ШИФРОВАНИЯ СТАНДАРТ ISO/IEC 10116:1997

В 1991 году был представлен стандарт ISO/IEC 10118, а версия 1997 года является второй редакцией, содержащей слегка расширенную версию CFB режима.

СТАНДАРТЫ (NBS, ANSI, ISO) СОДЕРЖАТ ЧЕТЫРЕ РАБОЧИХ РЕЖИМА:
– режим электронной кодовой книги (Electronic Code Book Mode, ECB);
– режим сцепления блоков текста (Cipher Block Chaining Mode, CBC);
– режим обратной связи по шифртексту (Ciphertext Feed Back Mode CFB);
– режим обратной связи по выходу (Output Feed Back Mode, OFB).

Символ E - операция шифрования n-битного блочного шифра, где n – количество бит в блоках открытого и закрытого текстов.
Символом D - операция расшифрования для того же шифра.

Преобразование открытого текста P в закрытый текст C осуществляется по формуле: $C = E_k(P)$,

где C- n-битный блок шифртекста;
K-секретный ключ для блочного шифра;
P- n-битный блок открытого текста.

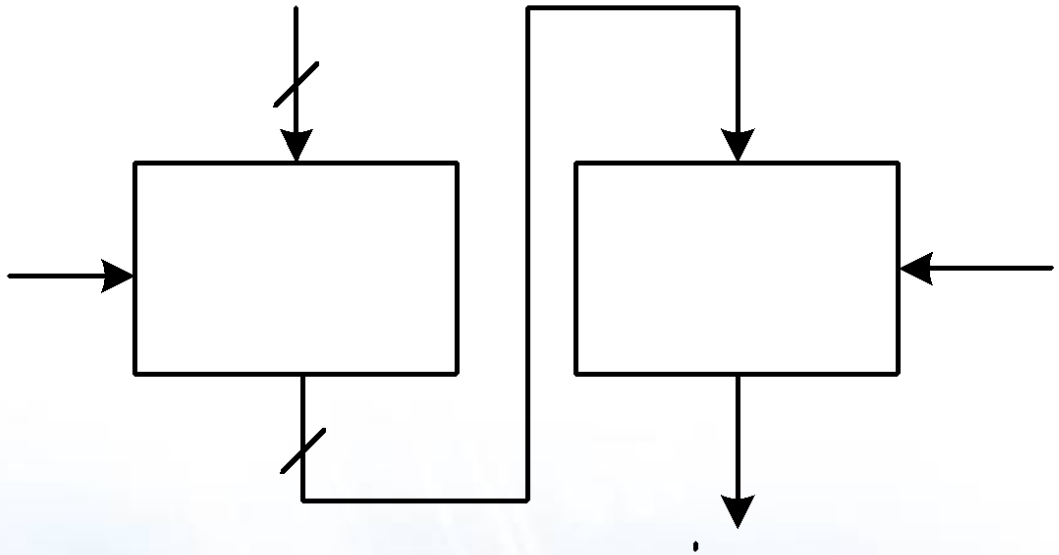
Аналогичным образом имеем обратное преобразование:

$$P=D_k(C),$$

а также справедливо соотношение вида:

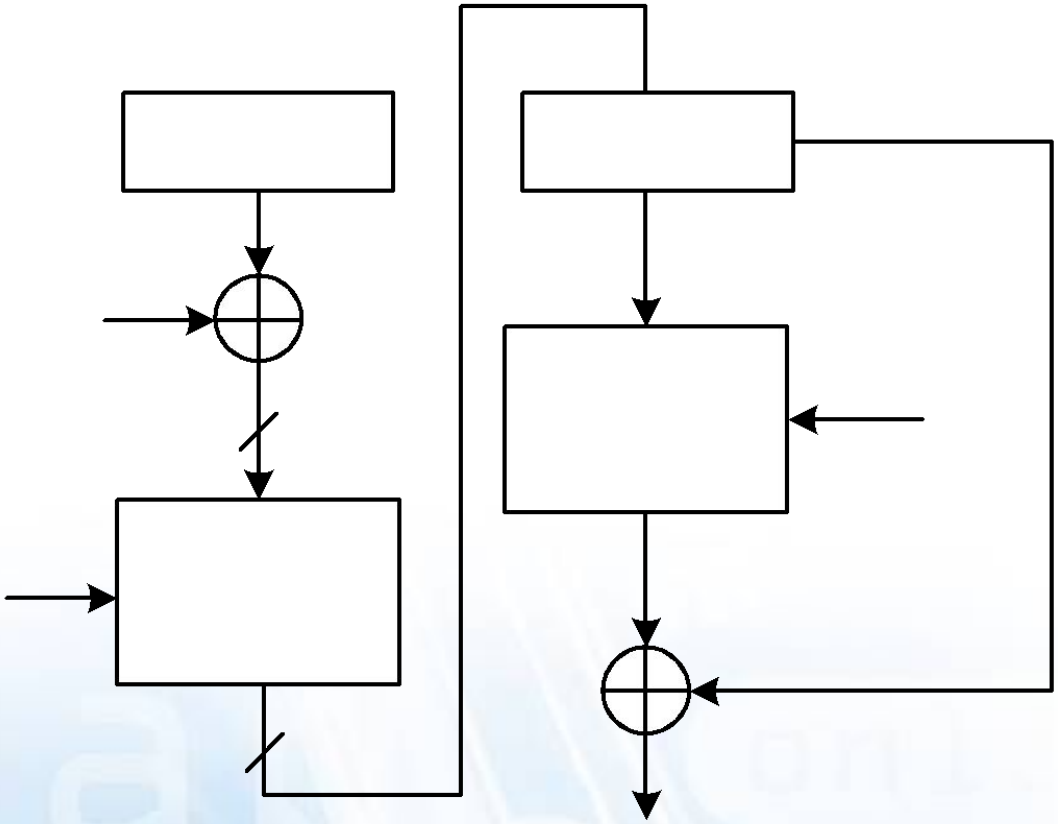
$$P=D_k(E_k(P)).$$

РЕЖИМ ЭЛЕКТРОННОЙ КОДОВОЙ КНИГИ (ELECTRONIC CODE BOOK MODE)



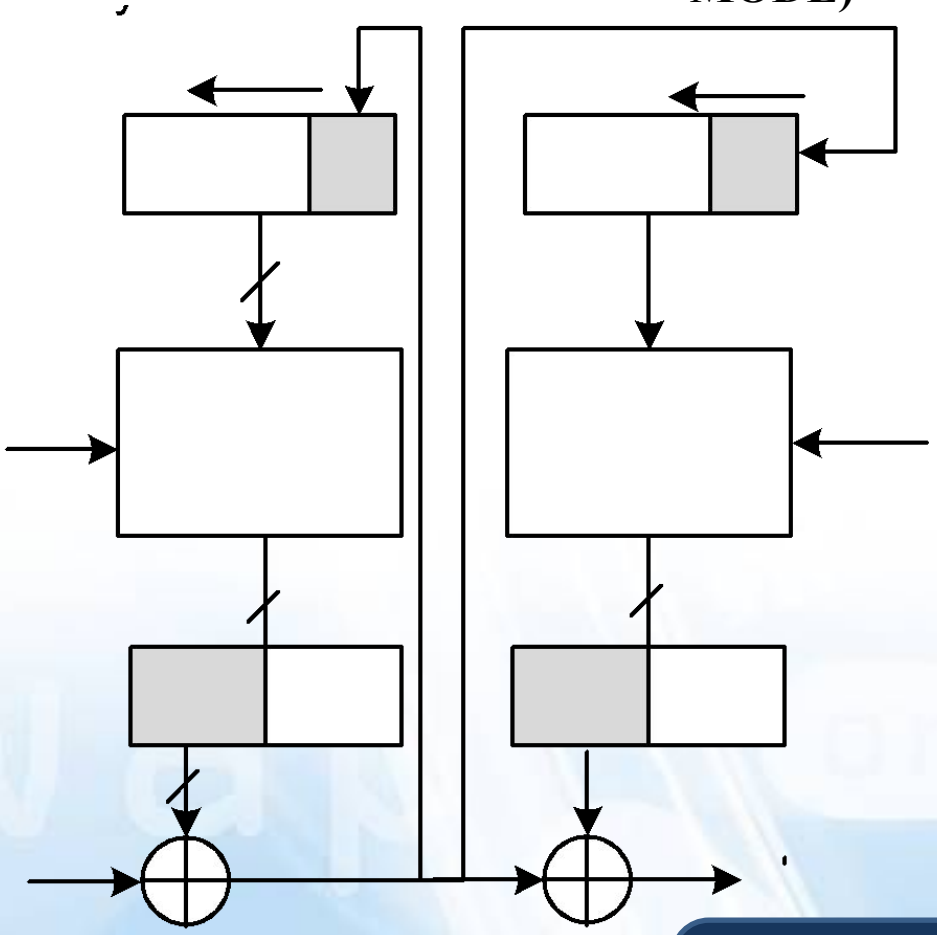
Достоинства: простота реализации, возможность распараллеливания режима шифрования.
Недостатки: низкий уровень криптостойкости

РЕЖИМ СЦЕПЛЕНИЯ БЛОКОВ ТЕКСТА (CIPHER BLOCK CHAINING MODE)



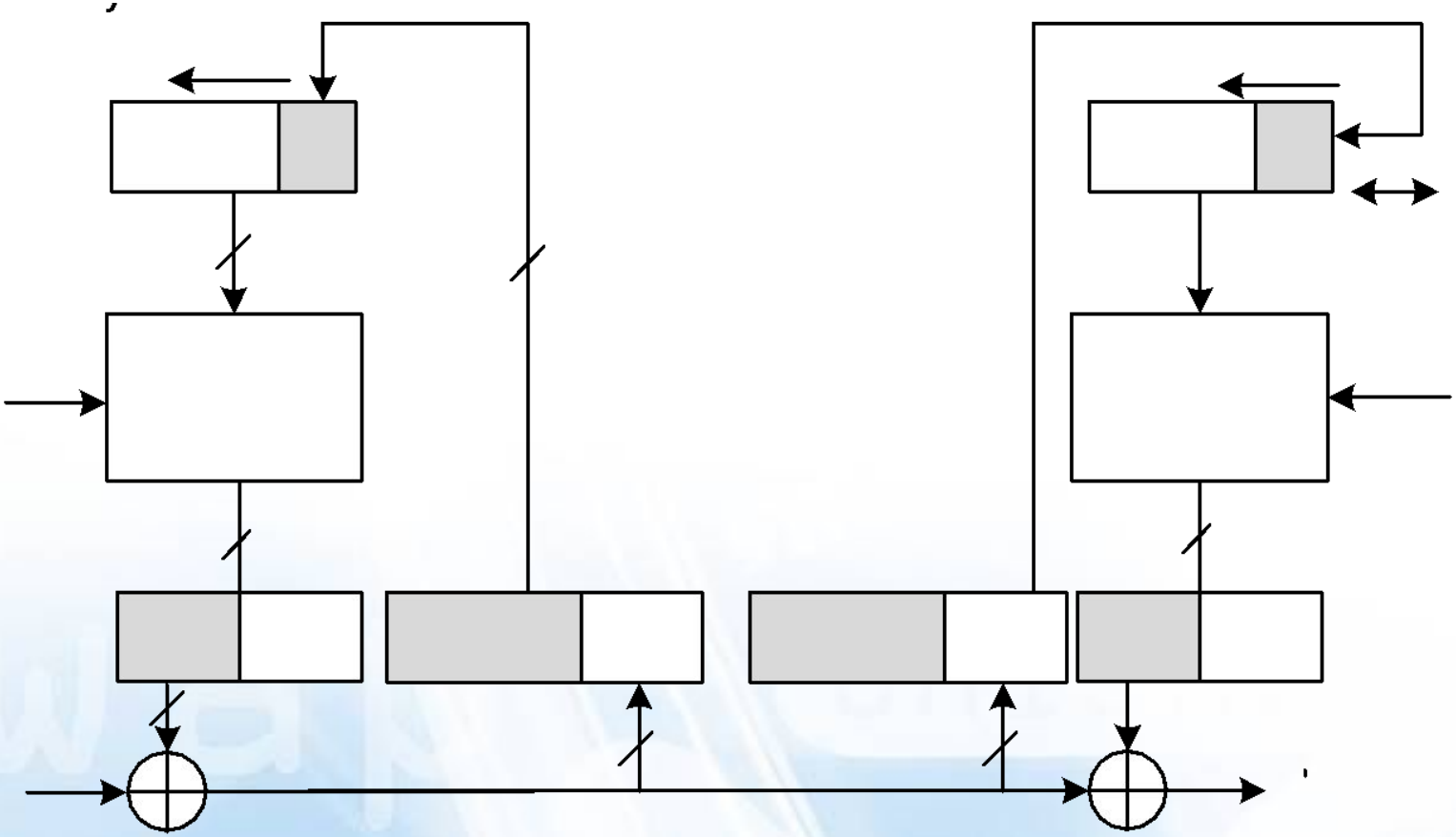
Достоинства: формирование MAC-кодов.
Недостатки: возможность распространения ошибки на весь блок криптограммы

РЕЖИМ ОБРАТНОЙ СВЯЗИ ПО ШИФРТЕКСТУ (CIPHERTEXT FEED BACK MODE)



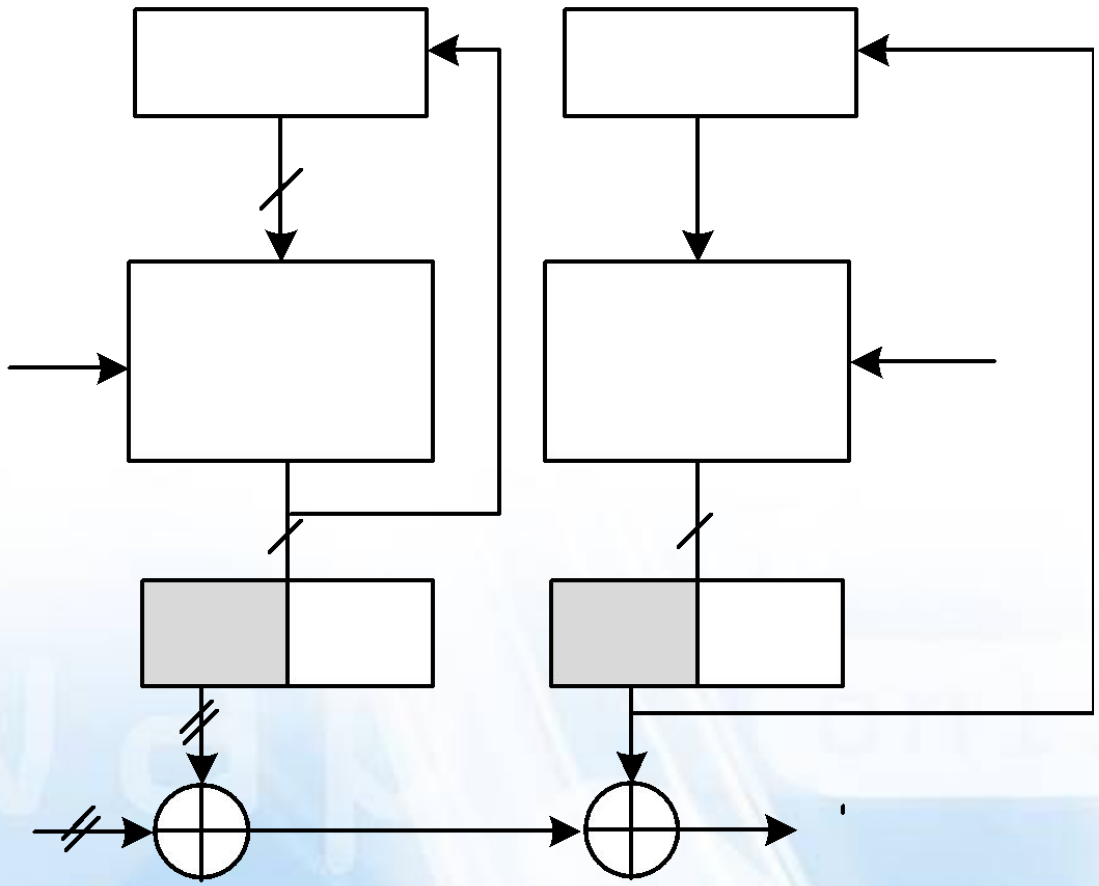
Достоинства: формирование MAC-кодов.
Недостатки: низкая скорость шифрования

РЕЖИМ ОБРАТНОЙ СВЯЗИ ПО ШИФРТЕКСТУ (CIPHERTEXT FEED BACK MODE) усовершенствованный



Достоинства: формирование MAC-кодов.
Недостатки: низкая скорость шифрования

РЕЖИМ ОБРАТНОЙ СВЯЗИ ПО ВЫХОДУ(OUTPUT FEED BACK MODE)



Достоинства: обеспечение максимальной криптостойкости.
Недостатки: низкая скорость шифрования

АСИММЕТРИЧНЫЕ СХЕМЫ ШИФРОВАНИЯ

Требования к алгоритму шифрования с открытым ключом:

- Вычислительно легко создавать пару (открытый ключ KU, закрытый ключ KR).
- Вычислительно легко, имея открытый ключ и незашифрованное сообщение M, создать соответствующее зашифрованное сообщение:

$$C = E_{KU}[M]$$

- Вычислительно легко расшифровать сообщение, используя закрытый ключ:

$$M = D_{KR}[C] = D_{KR}[E_{KU}[M]]$$

- Вычислительно невозможно, зная открытый ключ KU, определить закрытый ключ KR.
- Вычислительно невозможно, зная открытый ключ KU и зашифрованное сообщение C, восстановить исходное сообщение M.
- Шифрующие и расшифрующие функции могут применяться в любом порядке:

$$M = E_{KU}[D_{KR}[M]]$$

Односторонней функцией называется такая функция, у которой каждый аргумент имеет единственное обратное значение, при этом вычислить саму функцию легко, а вычислить обратную функцию трудно.

$$Y = f(X) \text{ –легко, } X = f^{-1}(Y) \text{ – трудно}.$$

NP-полные ЗАДАЧИ

ФАКТОРИЗАЦИЯ ЧИСЛА

Разложение n на два простых сомножителя:

$$p \times g = n$$

Лучший из известных алгоритмов взлома дает результат, пропорциональный:

$$L(n) = e^{\text{sqrt}(\ln n * \ln(\ln n))}$$

Если будет найден алгоритм, решающий некоторую (любую) NP-полную задачу за полиномиальное время, то все NP-задачи окажутся в классе P, то есть будут решаться за полиномиальное время.

ДИСКРЕТНЫЙ ЛОГАРИФМ В ГРУППЕ ЧИСЕЛ

A – примитивный корень простого числа Q как числа, чьи степени создают все целые от 1 до Q – 1.

$A \bmod Q, A^2 \bmod Q, \ldots, A^{Q-1} \bmod Q$

Для любого целого Y < Q и примитивного корня A можно найти единствен- ную экспоненту X:

$$Y = A^X \bmod Q,$$

где $0 \le X \le (Q - 1)$

$$X = \text{ind}_{A,Q}(Y).$$

ДИСКРЕТНЫЙ ЛОГАРИФМ В ГРУППЕ ТОЧЕК ЭЛЛЕПТИЧЕСКОЙ КРИВОЙ

Рассматривается группа точек ЭК над конечным полем. В данной группе определена операция сложения двух точек. Нахождение такого натурального числа m, что **mP = A** для заданных точек P и A.

ДЕКОДИРОВАНИЕ СЛУЧАЙНОГО КОДА

Нахождение **(n, k, d)** – параметров, где
n – длина кодовой последовательности;
k – длина инф. последовательности;
d – конструктивное кодовое расстояние.

В теории алгоритмов NP-полная задача — задача из класса NP, к которой можно свести любую другую задачу из класса NP за полиномиальное время.

АСИММЕТРИЧНАЯ СИСТЕМА RSA

p, q - два простых целых числа	- открыто, вычисляемо.
$n = p \cdot q$	- закрыто, вычисляемо.
d, $\gcd(\Phi(n), d) = 1$; $1 < d < \Phi(n)$	- открыто, выбираемо.
$d\ e^{-1} \equiv \mod \Phi(n)$	- закрыты, выбираемы.

Создание ключей

Выбрать простые p и q
Вычислить $n = p \cdot q$
Выбрать d $\gcd(\Phi(n), d) = 1; 1 < d < \Phi(n)$
Вычислить e $e = d^{-1} \mod \Phi(n)$
Открытый ключ KU = {e, n}
Закрытый ключ KR = {d, n}

Шифрование

Незашифрованный текст: $M < n$
Зашифрованный текст: $C = M^e \pmod n$

Расшифрование

Зашифрованный текст: C
Незашифрованный текст: $M = C^d \pmod n$

Алгоритм разработан в 1977 году Роном Ривестом, Ади Шамиром и Леном Адлеманом (алгоритм Rivest-Shamir-Adleman (RSA)).

АСИММЕТРИЧНАЯ СИСТЕМА ОБМЕНА КЛЮЧАМИ ДИФФИ-ХЕЛЛМАНА

Общеизвестные элементы	
q	простое число
p	p < q и p является примитивным корнем q
Создание пары ключей пользователем А	
Выбор случайного числа x (закрытый ключ, KR)	x < q
Вычисление числа X (открытый ключ, KU)	$X = p^x \bmod q$

Абонент А

Общеизвестные элементы	
q	простое число
p	p < q и p является примитивным корнем p
Создание пары ключей пользователем В	
Выбор случайного числа y (закрытый ключ, KR)	y < q
Вычисление числа Y (открытый ключ, KU)	$Y = p^y \bmod q$

Абонент В

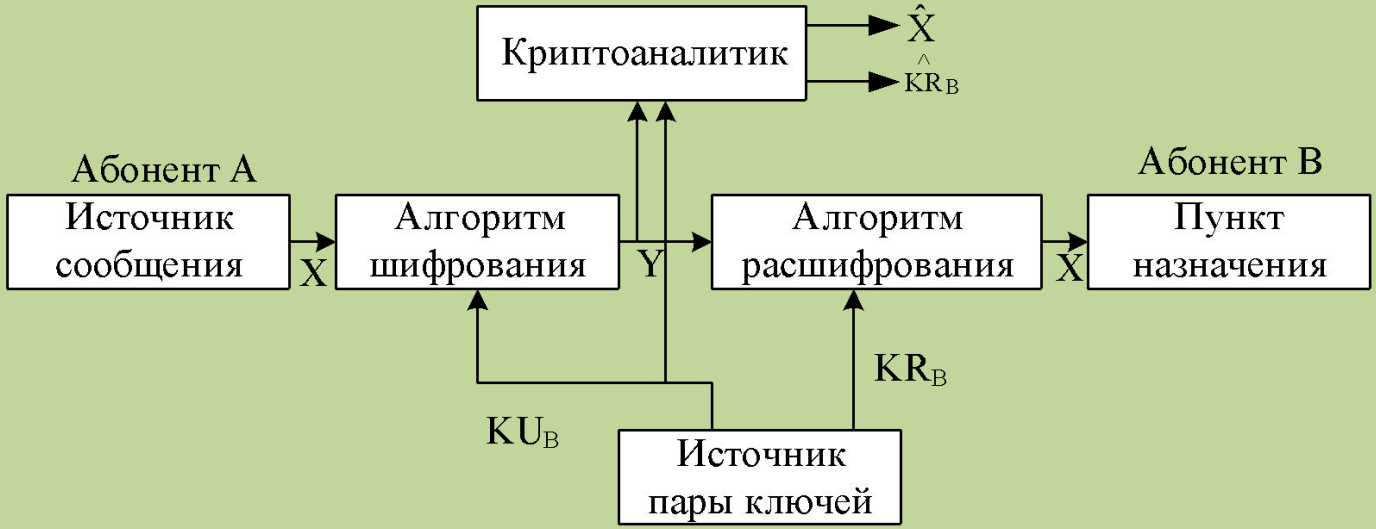
Создание общего секретного ключа пользователем А
$\mathbf{K = (Y)^x \bmod Q}$
Создание общего секретного ключа пользователем В
$\mathbf{K = (X)^y \bmod Q}$

Обмен секретными ключами

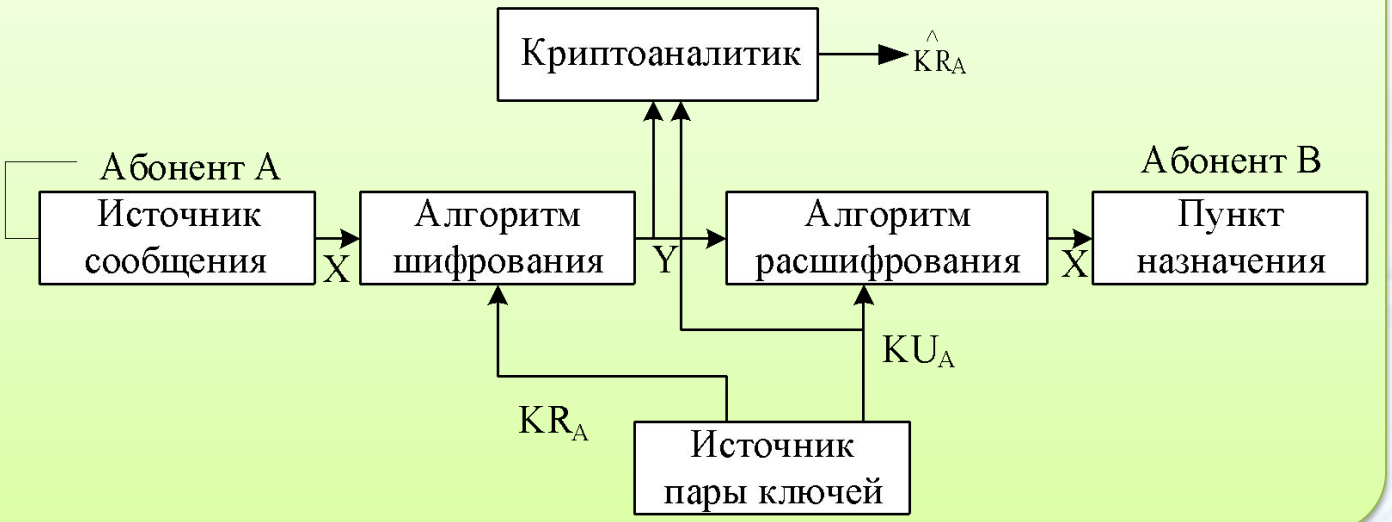
Алгоритм основан на трудности вычислений дискретных логарифмов и уязвим для атак типа "man-in-the-middle".

АСИММЕТРИЧНАЯ СИСТЕМА RSA

Протокол обеспечения конфиденциальности



Протокол обеспечения аутентичности



АСИММЕТРИЧНАЯ СИСТЕМА RSA

Протокол обеспечения аутентичности и конфиденциальности