Блок А: ШИФРЫ ОДНОЗНАЧНОЙ ЗАМЕНЫ

1. Шифр простой замены АТБАШ

читается справа налево					
Далет ד	Гимель ג	Бет ב	Алеф א		
Йод י	Тет ט	Хет ח	Заин ז	Вав ו	Хей ה
Аин ע	Самех ס	Нун נן	Мем מם	Ламед ל	Каф כך
Тав ת	Шин ש	Реш ר	Куф ק	Цади צץ	Пе פף

$$Y_i = X_{(n-i+1)}$$

X – исходный (открытый) текст
Y– зашифрованный текст
i – порядковый номер буквы в открытом алфавите, i=1…n
n – количество букв в открытом алфавите.

Y	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П
X	Я	Ю	Э	Ь	Ы	Ъ	Щ	Ш	Ч	Ц	Х	Ф	У	Т	С	Р
i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Y	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
X	П	О	Н	М	Л	К	Й	И	З	Ж	Е	Д	Г	В	Б	А
i	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32

2. ШИФР ЦЕЗАРЯ

Цезарь Гай Юлий (100-44 гг. до н.э.), полководец, римский император

$$\mathbf{Y_i = X_{i+3} \bmod n}$$

X – исходный (открытый) текст
Y– зашифрованный текст
i – порядковый номер буквы открытого текста в алфавите, i=(1…n)
n – количество букв в выбранном алфавите (мощность алфавита).

X	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П
Y	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т
i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

X	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
Y	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В
i	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32

3. Квадрат Полибия

Шифр замены, называемый **Квадратом Полибия**, был изобретен во 2 веке до нашей эры, он использовался для предупреждения об опасности с помощью двух факелов с охранных постов.

Текст алфавита помещается в таблицу, где каждой букве соответствуют два числа – номер строки i (количество факелов в левой руке) и номер столбца j (количество факелов в правой руке).

	1	2	3	4	5	6
1	А	Б	В	Г	Д	Е
2	Ж	З	И	Й	К	Л
3	М	Н	О	П	Р	С
4	Т	У	Ф	Х	Ц	Ч
5	Ш	Щ	Ъ	Ы	Ь	Э
6	Ю	Я	-			

Шифрование производится по формуле:

$$Y_{ij} = ij$$

Где:
Y – исходный (открытый) текст
ij – зашифрованный текст
i – номер строки
j – номер столбца

Например, букве «И» соответствует число 23, где 2 – номер строки, 3 – номер столбца.

Таким образом, половица

Выпущенное слово и камень не имеют возврата

в зашифрованном виде выглядит так:

13 54 34 42 52 16 32 32 33 16 36 26 33 13 33 23 25 11 31 16 32 55 32 16 23 31 16 61 41 13 33 22 13 35 11 41 11

Блок В: ШИФРЫ МНОГОЗНАЧНОЙ ЗАМЕНЫ

4. Шифр Тритемия

В Германии XV-XVI веках значительный вклад в криптографию внёс **Иоганнес Тритемий**, аббат монастыря в городе Вюрцбург, находившийся под личным покровительством императора Максимилиана I, написал в 1499г. и издал в **1518**г. книгу «**Полиграфия**» - *первую печатную книгу* по криптографии.

$$Y_j = X_{i+j-1} \bmod n$$

X – исходный (открытый) текст
Y– зашифрованный текст
i – порядковый номер буквы в алфавите таблицы, i=1…n
j – порядковый номер буквы в тексте, j=1…k
k – количество букв в тексте
n – количество букв в выбранном алфавите (мощность алфавита).

ТАБЛИЦА ТРИТЕМИЯ

A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	X	Y	Z	W
B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	X	Y	Z	W	A
C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	X	Y	Z	W	A	B
D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	X	Y	Z	W	A	B	C
E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	X	Y	Z	W	A	B	C	D
F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	X	Y	Z	W	A	B	C	D	E
G	H	I	K	L	M	N	O	P	Q	R	S	T	U	X	Y	Z	W	A	B	C	D	E	F
H	I	K	L	M	N	O	P	Q	R	S	T	U	X	Y	Z	W	A	B	C	D	E	F	G
I	K	L	M	N	O	P	Q	R	S	T	U	X	Y	Z	W	A	B	C	D	E	F	G	H
K	L	M	N	O	P	Q	R	S	T	U	X	Y	Z	W	A	B	C	D	E	F	G	H	I
L	M	N	O	P	Q	R	S	T	U	X	Y	Z	W	A	B	C	D	E	F	G	H	I	K
M	N	O	P	Q	R	S	T	U	X	Y	Z	W	A	B	C	D	E	F	G	H	I	K	L
N	O	P	Q	R	S	T	U	X	Y	Z	W	A	B	C	D	E	F	G	H	I	K	L	M
O	P	Q	R	S	T	U	X	Y	Z	W	A	B	C	D	E	F	G	H	I	K	L	M	N
P	Q	R	S	T	U	X	Y	Z	W	A	B	C	D	E	F	G	H	I	K	L	M	N	O
Q	R	S	T	U	X	Y	Z	W	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P
R	S	T	U	X	Y	Z	W	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q
S	T	U	X	Y	Z	W	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R
T	U	X	Y	Z	W	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S
U	X	Y	Z	W	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T
X	Y	Z	W	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U
Y	Z	W	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	X
Z	W	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	X	Y
W	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	X	Y	Z

Это первый **многоалфавитный периодический шифр**

5. Шифр Белазо

Джованни Батиста **Белазо** в **1553** году (брошюра «Шифр синьора Белазо») предложил использовать для **многоалфавитного шифра** буквенный, легко запоминаемый ключ, который он назвал ***паролем***.

Шифрование осуществляется с помощью пароля-ключа, состоящего из М символов. Из полной таблицы Тритемия выделяется матрица $T_Ш$ размерностью [(М+1) x R]. Она включает первую строку и строки, первые элементы которых совпадают с символами ключа. Если в качестве ключа выбрано слово <ЗОНД>, то матрица шифрования содержит пять строк :

	А	Б	В	Г	Д	Е	Ж	З	И	К	.	.	.	Э	Ю	Я	␣
	З	И	К	Л	М	Н	О	П	Р	С	.	.	.	Г	Д	Е	Ж
$T_В$=	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	.	.	.	К	Л	М	Н
	Н	О	П	Р	С	Т	У	Ф	Х	Ц	.	.	.	И	К	Л	М
	Д	Е	Ж	З	И	К	Л	М	Н	О	.	.	.	А	Б	В	Г

Замена с использованием шифра Белазо эквивалентна простой замене с циклическим изменением алфавита. При этом в каждом цикле имеем многоалфавитную подстановку с числом используемых алфавитов, соответствующим числу букв в слове ключа.

При шифровании необходимо вначале записать под буквами шифруемого текста буквы ключевого слова. Ключ при этом повторяется необходимое число раз. Символ шифруемого текста определяет столбец матрицы шифрования. Необходимый для его замены символ находится на пересечении этого столбца со строкой, соответствующей букве ключа, записанного под шифруемым текстом.

В примере шифрования с помощью шифра Белазо шифруется слово <КРИПТОГРАФИЯ>. Процесс шифрования осуществляется следующим образом:

1. под шифруемым словом записываем нужное число раз ключевое слово <ЗОНД>;
2. берем первую букву шифруемого слова (К) и соответствующую ей букву ключа (З);
3. по букве К входим в соответствующий столбец матрицы шифрования (рис. 6.6);
4. выбираем в этом столбце букву, расположенную в строке, соответствующей букве ключа (З).

В нашем примере такой буквой является буква С, которая помещается в шифрованный текст в качестве символа замены исходной буквы К. Данная процедура циклически повторяется до завершения шифрования всего слова. В результате получает шифрованное слово <СЭХУЩЫРФЗАХВ>.

Пример шифрования с помощью пароля-ключа:

Исходное слово	К	Р	И	П	Т	О	Г	Р	А	Ф	И	Я
Ключ	З	О	Н	Д	З	О	Н	Д	З	О	Н	Д
Шифрованное слово методом замены	С	Э	Х	У	Щ	Ы	Р	Ф	З	А	Х	В

6. Шифр Виженера

Блез де Виженер

В книге "Трактат о шифрах" Блез де Виженер описал два шифра, работающих по принципу шифра Белазо (см. выше), но в качестве пароля используется сам шифруемый текст с добавленной перед ним секретной буквой:

1.Шифр с самоключом

$$\Gamma = t_0 t_1 t_2 \ldots t_{i-1} \ldots$$
$$T_O = t_1 t_2 t_3 \ldots t_i \ldots$$
$$T_ш = s_1 s_2 s_3 \ldots s_i \ldots$$

T_O – открытый текст
Г - гамма, накладываемая на текст (по модулю мощности алфавита)
$T_ш$ – шифртекст
t_i , s_i – буквы используемого алфавита в тексте и шифртексте
i – порядковый номер буквы в тексте или шифртексте.

2.Шифр ключом-шифртекстом

$$\Gamma = s_o s_1 s_2 \ldots s_{i-1} \ldots$$
$$T_O = t_1 t_2 t_3 \ldots t_i \ldots$$
$$\_\_\_\_\_$$
$$T_ш = s_1 s_2 s_3 \ldots s_i \ldots$$

7. S-блок замены ГОСТ Р 34.12-2015 («МАГМА»)

В отличие от ГОСТ 28147-89, в котором заполнение узлов замены (S-блоков) производилось разработчиками СКЗИ, шифр «Магма» (ГОСТ Р 34.12-2015) содержит единственный у*зел замены, определенный Техническим комитетом по стандартизации "Криптографическая защита информации" (ТК 26):*

Номер S-блока	**Значение**															
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
1	C	4	6	2	A	5	B	9	E	8	D	7	0	3	F	1
2	6	8	2	3	9	A	5	C	1	E	4	7	B	D	0	F
3	B	3	5	8	2	F	A	D	E	1	7	4	C	9	6	0
4	C	8	2	1	D	4	F	6	7	0	A	5	3	E	9	B
5	7	F	5	A	8	1	6	D	0	9	3	E	B	4	2	C
6	5	D	F	6	9	2	C	A	B	7	8	1	4	3	E	0
7	8	E	2	5	6	9	1	C	F	4	B	0	D	A	3	7
8	1	7	E	D	0	5	8	3	4	F	A	6	9	C	B	2

Используемый набор подстановок был выбран исходя из обеспечения наилучших характеристик, определяющих невозможность применения дифференциального и линейного методов криптографического анализа. Данный узел замен предлагался ТК 26 при международной стандартизации ГОСТ 28147-89 в составе стандарта шифрования ISO/IEC 18033-3 и рекомендовался отечественным разработчикам СКЗИ.

Фиксированный набор подстановок позволит максимально упростить разработку взаимодействующих информационно-телекоммуникационных систем.

Блок в 32 бита разбивается на восемь 4-битовых подпоследовательностей, каждая из которых поступает на вход своего S-блока. Общее количество S-блоков ГОСТа — восемь, т. е. столько же, сколько и подпоследовательностей. Каждый S-блок представляет собой перестановку чисел от 0 до 15. Первая 4-битная подпоследовательность попадает на вход первого S-блока, вторая — на вход второго и т. д.

Если S-блок выглядит так:
1, 15, 13, 0, 5, 7, 10, 4, 9, 2, 3, 14, 6, 11, 8, 12
и на входе S-блока 0, то на выходе будет 1, если 5, то на выходе будет 7 и т. д.
Выходы всех восьми S-блоков объединяются в 32-битное слово,
(в криптосистеме ГОСТ Р 34.12-2015 всё слово циклически сдвигается влево на 11 бит).

Блок С: ШИФРЫ БЛОЧНОЙ ЗАМЕНЫ

8. Матричный шифр

Предполагается, что буквы занумерованы от 0 до 32 и рассматриваются как элементы некоторого алгебраического кольца. Если к n-грамме сообщения применить матрицу a_{ij}, то получится n-грамма криптограммы

$$l_i = \sum_{j=1}^{n} a_{ij} m_j, \qquad i = 1, \ldots, n.$$

Матрица a_{ij} является ключом, и расшифровка выполняется с помощью обратной матрицы.

Обратная матрица будет существовать тогда и только тогда, когда определитель $|a_{ij}|$ имеет обратный элемент в кольце.

В качестве матричного шифрования информации могут использоваться аналитические преобразования, основанные, на преобразованиях матричной алгебры.

Шифрование k-ого блока исходной информации, представленного в виде вектора $B_k = \|b_j\|$, осуществляется путем перемножения этого вектора на матрицу $A = \|a_{ij}\|$, используемую в качестве ключа. В результате перемножения получается блок шифротекста в виде вектора $C_k = \|c_i\|$, где элементы вектора C_k определяются по формуле:

$$C_i = \sum_j a_{ij} b_j .$$

Приведем пример, взяв в качестве ключа квадратную матрицу третьего порядка: $A = \begin{vmatrix} 1 & 4 & 8 \\ 3 & 7 & 2 \\ 6 & 9 & 5 \end{vmatrix}$.

Пусть требуется с помощью этого ключа зашифровать слово

$$T_0 = \langle \textit{ЗАБАВА} \rangle .$$

Для этого необходимо выполнить следующие шаги.

1. Определяется числовой эквивалент $T_Э$ исходного слова как последовательность соответствующих порядковых номеров букв этого слова в алфавите:

$$T_Э = <8,1,2,1,3,1>.$$

2. Умножается ключевая матрица A на векторы $B_1 = \{8,1,2\}$ и $B_2 = \{1,3,1\}$:

$$C_1 = \begin{vmatrix} 1 & 4 & 8 \\ 3 & 7 & 2 \\ 6 & 9 & 5 \end{vmatrix} \cdot \begin{vmatrix} 8 \\ 1 \\ 2 \end{vmatrix} = \begin{vmatrix} 28 \\ 35 \\ 67 \end{vmatrix};$$

$$C_2 = \begin{vmatrix} 1 & 4 & 8 \\ 3 & 7 & 2 \\ 6 & 9 & 5 \end{vmatrix} \cdot \begin{vmatrix} 1 \\ 3 \\ 1 \end{vmatrix} = \begin{vmatrix} 21 \\ 26 \\ 38 \end{vmatrix}.$$

3. Зашифрованное слово записывается в виде последовательности чисел

$$T_1 = <\boldsymbol{28,35,67,21,26,38}>.$$

Расшифрование осуществляется также с использованием правил матричной алгебры, только в качестве ключа берется матрица, обратная той, с помощью которой осуществлялось шифрование, а в качестве вектора-сомножителя – соответствующие фрагменты символов зашифрованного текста. Тогда компонентами вектора-результата будут цифровые эквиваленты букв открытого текста.

Для расшифрования полученной в предыдущем примере последовательности чисел T_1 необходимо выполнить следующие шаги.

1. Вычисляется определитель матрицы-ключа $|A| = -115$.

2. Находится присоединенная матрица $A^* = \begin{vmatrix} 17 & -3 & -15 \\ 52 & -43 & 15 \\ -48 & 22 & -5 \end{vmatrix}$, каждый элемент a^*_{ij} которой является алгебраическим дополнением элемента a_{ij} матрицы-ключа A, то есть $a^*_{ij} = (-1)^{i+j}\Delta_{ij}$, где Δ_{ij} - определитель матрицы, получаемой вычеркиванием i-й строки и j-ого столбца исходной матрицы A.

3. Получается транспонированная матрица $A^m = \begin{vmatrix} 17 & 52 & -48 \\ -3 & -43 & 22 \\ -15 & 15 & -5 \end{vmatrix}$, элементы которой $a^m_{ij} = a^*_{ji}$.

4. Вычисляется обратная матрица $A^{-1} = \begin{vmatrix} -17/115 & -52/115 & 48/115 \\ 3/115 & 43/115 & -22/115 \\ 15/115 & -15/115 & 5/115 \end{vmatrix}$,

элементы которой $a_{ij}^{-1} = a_{ij}^{*} / |A|$.

5. Определяются векторы $B_1 = A^{-1}C_1$ и $B_2 = A^{-1}C_2$:

$$B_1 = \begin{vmatrix} -17/115 & -52/115 & 48/115 \\ 3/115 & 43/115 & -22/115 \\ 15/115 & -15/115 & 5/115 \end{vmatrix} \cdot \begin{vmatrix} 28 \\ 35 \\ 67 \end{vmatrix} = \begin{vmatrix} 8 \\ 1 \\ 2 \end{vmatrix};$$

$$B_2 = \begin{vmatrix} -17/115 & -52/115 & 48/115 \\ 3/115 & 43/115 & -22/115 \\ 15/115 & -15/115 & 5/115 \end{vmatrix} \cdot \begin{vmatrix} 21 \\ 26 \\ 38 \end{vmatrix} = \begin{vmatrix} 1 \\ 3 \\ 1 \end{vmatrix}.$$

6. Числовой эквивалент расшифрованного слова $T_Э$ = <8,1,2,1,3,1> заменяется соответствующими символами алфавита, в результате чего получается исходное слово T_0 = <ЗАБАВА>.

9. Шифр Плэйфера – шифр биграммной замены

Система шифрования Плейфера была изобретена **Чарльзом Уитстоном,** который впервые описал её в 1854 году.
Лорд Лайон Плейфер, внес большой вклад в продвижение использования данной системы шифрования.

Биграммный шифр (Playfair, Великобритания), применявшийся Великобританией во время Первой мировой воны, был основан на ***лозунговом*** способе заполнения шифртаблицы.

Переход от биграмм входного текста к биграммам выходного текста осуществляется по следующим правилам: если буквы входной биграммы оказались в одном столбце таблицы, шифрование происходит сверху вниз; если же буквы входной биграммы оказались в одной строке таблицы, то шифрование осуществляется слева направо, а расшифрование — наоборот. Если буквы биграммы совпадают, их следует разделить буквой с наименьшей частотой встречаемости (например, Ф - для литературных текстов). Если буквы входной биграммы оказались в разных столбцах и строках таблицы, то рисуется воображаемый прямоугольник, а выходная биграмма берется как его альтернативные вершины.

Пример:
Открытый текст ***ПУСТЬ КОНСУЛЫ БУДУТ БДИТЕЛЬНЫ***, записанный без пробелов:
ПУСТЬКОНСУ ЛЫБУ ДУТБ ДИТЕ ЛЬНЫ,
имеет шифртекст:

УБ РХ ЫИ ДО ПБ КЩ РБ НР ШР ЖЛ ФР ИЩ ЗЮ

Пример использования шифра Плейфера (движение некоторых букв показано стрелками).

Блок D: ШИФРЫ ПЕРЕСТАНОВКИ

10. Вертикальная перестановка

Можно записать исходное сообщение в прямоугольную матрицу, выбрав такой маршрут: по горизонтали, начиная с левого верхнего угла поочередно слева направо и справа налево. Считывать же шифрованное сообщение по другому маршруту: по вертикали, начиная с правого верхнего угла и двигаясь поочередно сверху вниз и снизу вверх.

Зашифруем, например, таким способом фразу «пример маршрутной перестановки», используя прямоугольник размером 4 х 7 (рис.5.1):

Рис.5.1. Пример шифра маршрутной перестановки

	1	2	3	4	5	6	7
1	*П*	*Р*	*И*	*М*	*Е*	*Р*	*М*
2	*Н*	*Т*	*У*	*Р*	*Ш*	*Р*	*А*
3	*О*	*Й*	*П*	*Е*	*Р*	*Е*	*С*
4	*И*	*К*	*В*	*О*	*Н*	*А*	*Т*

Зашифрованная фраза выглядит так:

МАСТАЕРРЕШРНОЕРМИУПВКЙТРПНОИ.

Широко распространена разновидность шифра маршрутной перестановки, называемая *шифром вертикальной перестановки*. В таком шифре реализуется перестановка считываемых столбцов матрицы в соответствии с ключом. Пусть, например, этот ключ будет таким: 5,4,1,7,2,6,3. Теперь, выбирая столбцы в порядке, заданном ключом, и считывая последовательно буквы каждого из них сверху вниз, следующую криптограмму:

ЕШРНМРЕОПНОИМАСТРТЙКРРЕАИУПВ.

Ключом может быть слово. Например, *«ОКТЯБРЬ»*. Используя расположение букв этого ключа в алфавите, будем иметь набор чисел 3257146 – ключевую последовательность, аналогичную рассмотренной выше, но дающую новый шифртекст:

ЕШРНРТЙКПНОИРРЕАИУПВМАСТМРЕО.

Число ключей шифра вертикальной перестановки, независимо от способа задания, не более m!, где m – число столбцов таблицы шифрования.

11. Решетка Кардано

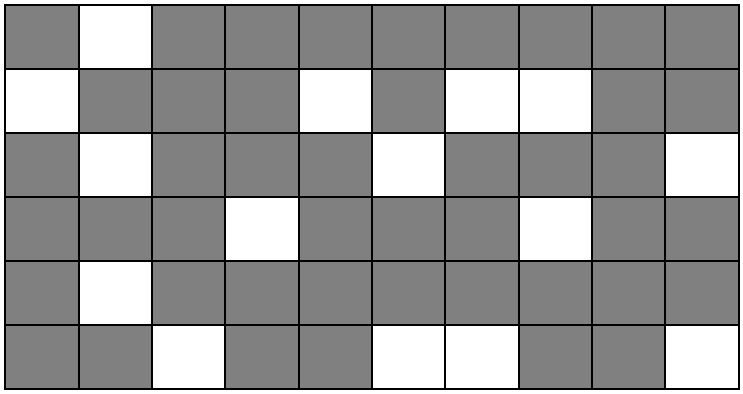
ПОВОРОТНЫЕ РЕШЕТКИ

или решетки Кардано по имени придумавшего их Дж.Кардано в XV веке

- *частный случай шифра маршрутной перестановки:*

используется трафарет из прямоугольного листа клетчатой бумаги размером **2m x 2k** клеток. В трафарете вырезано **m x k** клеток так, что при наложении его на чистый лист бумаги того же размера четырьмя возможными способами его вырезы полностью покрывают всю площадь листа.

Буквы сообщения последовательно вписываются в вырезы трафарета (по строкам, в каждой строке слева направо) при каждом из четырех его возможных положений в заранее установленном порядке.



Трафарет шифра «Поворотная решетка».

Число возможных трафаретов (т.е. количество ключей шифра «решетка») составляет

$$\mathbf{T = 4^{m \cdot k}}.$$

Уже при размерности решетки 8x8 число возможных решеток превосходит 4 миллиарда.

Текст: «***шифр решетка является частным случаем шифра маршрутной перестановки***».

а

	Ш								
И				Ф		Р	Р		
	Е				Ш				Е
			Т				К		
	А								
		Я			В	Л			Я

б

Е	*ш*		Т	С			Я		
И				Ф		Р	Р	Ч	
	Е	А			Ш	С			Е
Т			Т	Н			К	Ы	
	А	М	С		Л				У
		Я			В	Л		Ч	Я

в

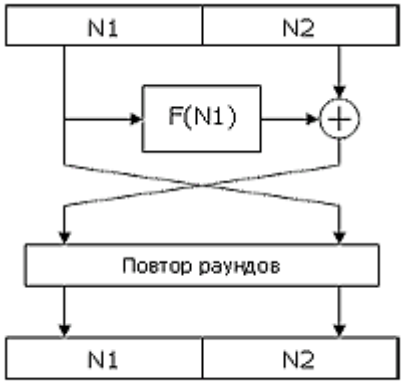
Е	*ш*	А	Т	С	Е	М	Я		Ш
И	И			Ф		Р	Р	Ч	
	Е	А	Ф		Ш	С	Р		Е
Т	А		Т	Н	М		К	Ы	А
Р	А	М	С	Ш	Л	Р	У		У
	Т	Я			В	Л		Ч	Я

г

Е	*ш*	А	Т	С	Е	М	Я	Н	Ш
И	И	О	Й	Ф	П	Р	Р	Ч	Е
Р	Е	А	Ф	Е	Ш	С	Р	С	Е
Т	А	Т	Т	Н	М	А	К	Ы	А
Р	А	М	С	Ш	Л	Р	У	Н	У
О	Т	Я	В	К	В	Л	И	Ч	Я

Рис.5.4. Последовательность использования поворотной решетки при шифровании.

12. Перестановка в комбинационных шифрах *(DES, ГОСТ 28147-89, МАГМА)*



В его основе лежит ***сеть Фейстеля*** - разновидность блочного шифра, предложенная в **1971 году Хорстом Фейстелем**. Для зашифрования открытый текст сначала разбивается на левую и правую половины L и R. На i-ом цикле используется подключ k_i:

$R_{i+1} = L_i$

$$L_{i+1} = R_i \oplus f(L_i, K_i)$$

где ($\oplus$ = xor)

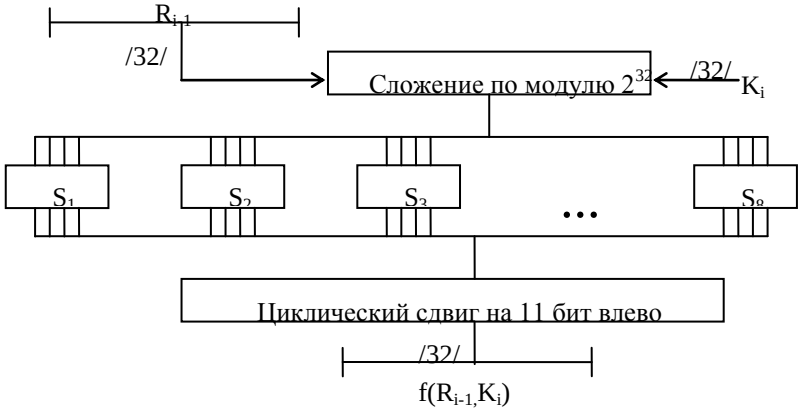
Для генерации подключей исходный 256-битный ключ разбивается на восемь 32-битных блоков: $K_1 \ldots K_8$.

Расшифрование выполняется так же, как и зашифрование, но инвертируется порядок подключей K_i.

Функция $f(L_i,K_i)$ вычисляется следующим образом:

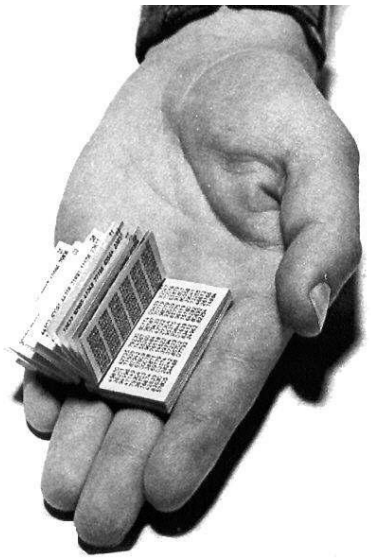
R_{i-1} и K_i складываются по модулю 2^{32}.

Результат разбивается на восемь 4-битовых подпоследовательностей, каждая из которых поступает на вход своего S-блока.



Блок-схема функции шифрования f алгоритмов ГОСТ 28147-89 и ГОСТ Р 34.12-2015 (Магма).

Блок E: ШИФРЫ ГАММИРОВАНИЯ



13. Одноразовый блокнот К.Шеннона

Популярность поточных шифров обязана анализу ***одноразовых гамма-блокнотов*** Клода Шеннона.

Название «одноразовый блокнот» стало общепринятым в годы Второй мировой войны, когда для шифрования широко использовались бумажные блокноты.

Открытый текст сообщения m записывают, как последовательность бит или символов $m = m_0 m_1 \ldots m_{n-1}$, а двоичную или символьную шифрующую последовательность k той же самой длины — как $k = k_0 k_1 \ldots k_{n-1}$.

Шифртекст $c = c_0 c1 \ldots c_{n-1}$ определяется соотношением $\mathbf{c_i = m_i} \oplus \mathbf{k_i}$ при $0 \le i \le n-1$, где $\oplus$ обозначает операцию «исключающее ИЛИ» (ассемблерная операция XOR) по модулю два или по любому другому модулю в случае символьной гаммы.

В своей исторической работе «Communication theory of secrecy systems» («Теория связи в секретных системах», 1949г.) Шеннон доказал то, что **одноразовый гамма-блокнот является «невскрываемой» шифрсистемой.**

В некоторых поточных шифрах ключ короче сообщения. Так, в системе Вернама для телеграфа используется бумажное кольцо, содержащее гамму. Конечно, стойкость такого шифра неидеальна.

14. Гаммирование ГОСТ 28147-89 и ГОСТ Р 34.13-2015 (ГОСТ Р 34.12-2015 «Магма»)

Схема реализации режима гаммирования приведена на рисунке 7.2.

Открытые данные, разбитые на 64-разрядные блоки $T_0^{(i)}$ зашифровываются в режиме гаммирования путем поразрядного суммирования по модулю 2 в сумматоре $СМ_5$ с гаммой шифра $Г_ш^{(i)}$, которая вырабатывается блоками по 64 бита. Число двоичных разрядов в блоке $T_0^{(M)}$, где М определяется объемом шифруемых данных может быть меньше 64, при этом неиспользованная для зашифрования часть гаммы шифра из блока $Г_ш^{(M)}$ отбрасывается.

В ключевое запоминающее устройство (КЗУ) вводятся 256 бит ключа. В накопители N_1, N_2 вводится 64-разрядная двоичная последовательность (*синхропосылка*) $S=(S_1,S_2,\ldots,S_{64})$, являющаяся исходным заполнением этих накопителей для последующей выработки М блоков гаммы шифра. Синхропосылка вводится в N_1 и N_2 так, что значение S_1 вводится в 1-ый разряд N_1, значение S_{33} – в 1-ый разряд N_2, S_{64} – в 32-й разряд N_2.

Исходное заполнение накопителей N_1 и N_2 (синхропосылка S) зашифровывается в режиме простой замены (нижняя часть рисунка). Результат зашифрования $A(S)=(Y_0,Z_0)$ переписывается в 32-разрядные накопители N_3 и N_4 так, что заполнение N_1 переписывается в N_3, а N_2 - в N_4.

Заполнение накопителя N_4 суммируется по модулю $(2^{32}-1)$ в сумматоре $СМ_4$ с 32-разрядной константой C_1 из накопителя N_6, результат записывается в N_4.

Заполнение накопителя N_3 суммируется по модулю 2^{32} в сумматоре $СМ_3$ с 32-разрядной константой C_2 из накопителя N_5, результат записывается в N_3.

Заполнение N_3 переписывается в N_1, а заполнение N_4 – в N_2. При этом заполнение N_3, N_4 сохраняется.

Заполнение N_1 и N_2 зашифровывается в режиме простой замены. Полученное в результате в N_1, N_2 зашифрование образует первый 64-рарядный блок гаммы шифра $Г_ш^{(1)}$, который суммируется в $СМ_5$ с первым 64- разрядным блоком открытых данных $T_0^{(1)}$.

В результате получается 64 – разрядный блок зашифрования данных $Г_ш^{(1)}$.

Для получения следующего 64-разрядного блока гаммы шифра $Г_ш^{(2)}$ заполнение N_4 суммируется по модулю $(2^{32}-1)$ в $СМ_4$. С константой C_1 из N_6, заполнение N_3 суммируется по модулю 2^{32} в сумматоре $СМ_3$ с C_2 (в N_5). Новое заполнение N_3 переписывается в N_1, а новое заполнение N_4 переписывается в N_2., при этом заполнение N_3, N_4 сохраняется.

Заполнение N_1 и N_2 зашифровывается в режиме простой замены. Полученное в результате зашифрования заполнение N_1, N_2 образует второй 64-разрядный блок гаммы шифра $Г_ш^{(2)}$, который поразрядно суммируется по модулю 2 в $СМ_5$ со вторым блоком открытых данных $T_0^{(2)}$.

Аналогично вырабатываются блоки гаммы шифра $Г_ш^{(3)}, \ldots, Г_ш^{(M)}$ и зашифровываются блоки открытых данных $T_0^{(3)}, \ldots, T_0^{(M)}$.

В канал связи (или память ЭВМ) передается синхропосылка S и блоки зашифрованных данных $T_ш^{(1)}, T_ш^{(2)}, \ldots, T_ш^{(M)}$.

Уравнение зашифрования имеет вид:

$T_ш^{(i)} = A(Y_{i-1} \boxplus C_2, Z_{i-} \boxplus' C_1) \oplus T_0^{(i)} = \Gamma_ш^{(i)} \oplus T_0^{(i)}$,

Где $\boxplus$ - суммирование по модулю 2^{32},

$\boxplus'$ – суммирование по модулю 2^{32}-1,

$\oplus$ - суммирование по модулю 2,

Y_i – содержимое накопителя N_3 после зашифрования i-го блока открытых данных $T_0^{(i)}$;

Z_i – содержимое накопителя N_4 после зашифрования i-го блока открытых данных $T_0^{(i)}$.

$(Y_0, Z_0) = A(S)$.

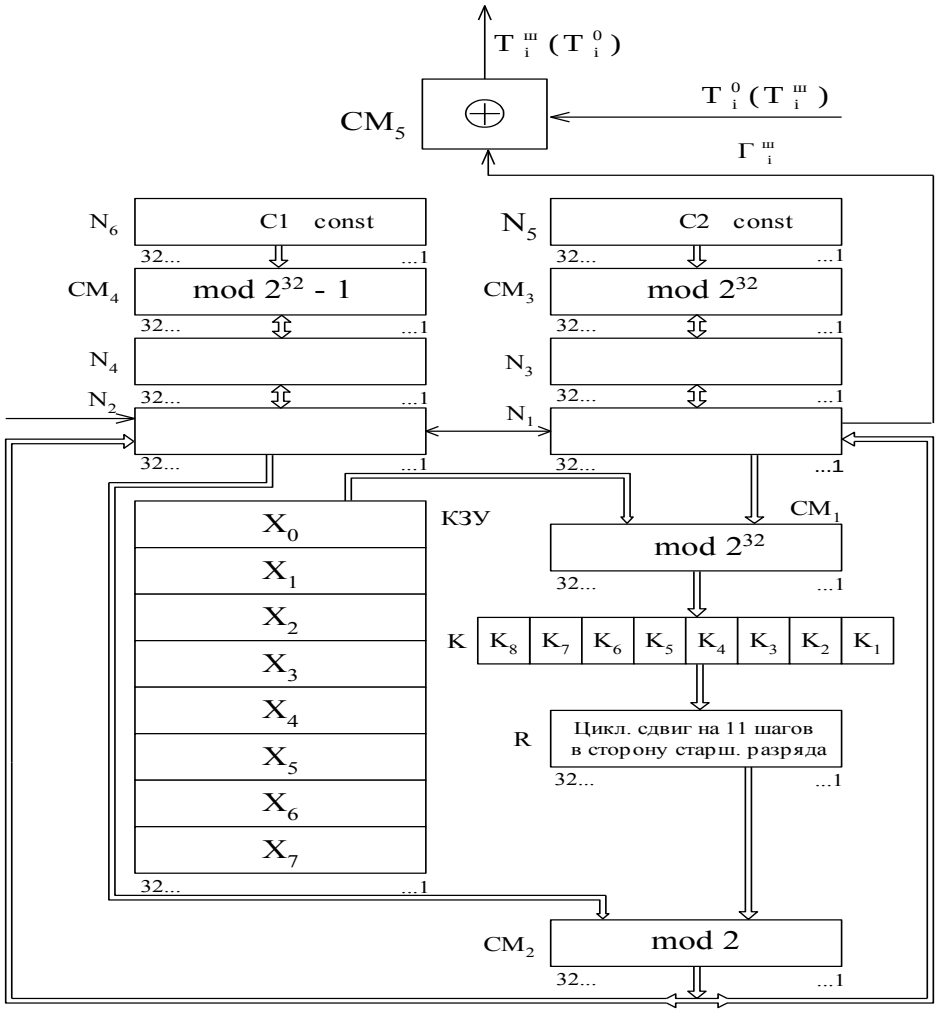
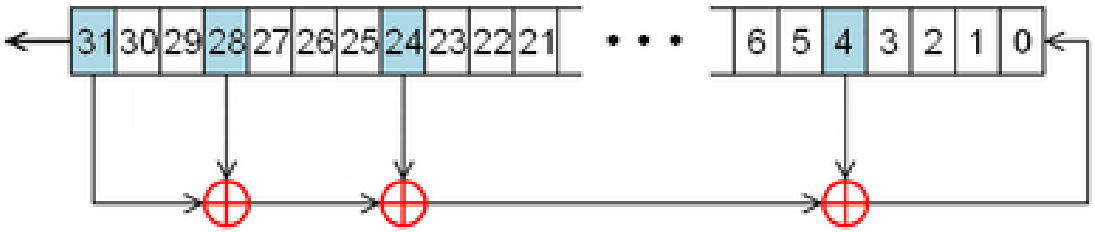


Рис.7.2. Режим гаммирования

Блок F: ПОТОЧНЫЕ ШИФРЫ

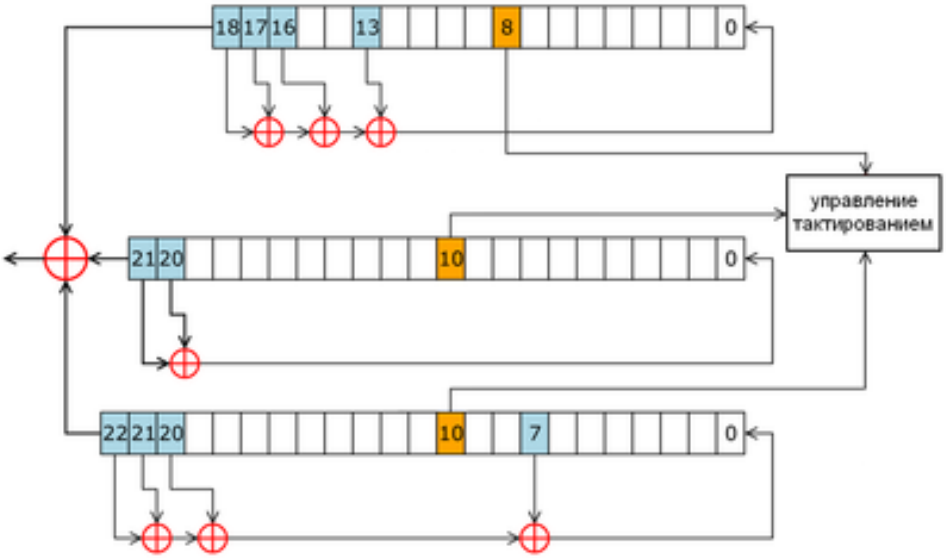
15.A5 /1
16. A5 /2

РАСЧЕТ РЕГИСТРОВ СДВИГА С ЛИНЕЙНОЙ ОБРАТНОЙ СВЯЗЬЮ
(РСЛОС)



Регистр сдвига с линейной обратной связью,
многочлен обратной связи $x^{32}+x^{29}+x^{25}+x^{5}+1$

АЛГОРИТМ ШИФРОВАНИЯ A5/1



Система РСЛОС в **алгоритме A5/1**:

Три регистра(R1, R2, R3) имеют длины 19, 22 и 23 бита,
Многочлены обратных связей:

$X^{19} + X^{18} + X^{17} + X^{14} + 1$ для R1
$X^{22} + X^{21} + 1$ для R2

$X^{23} + X^{22} + X^{21} + X^8 + 1$ для R3

Управление тактированием:

биты синхронизации: 8 (R1), 10 (R2), 10 (R3)

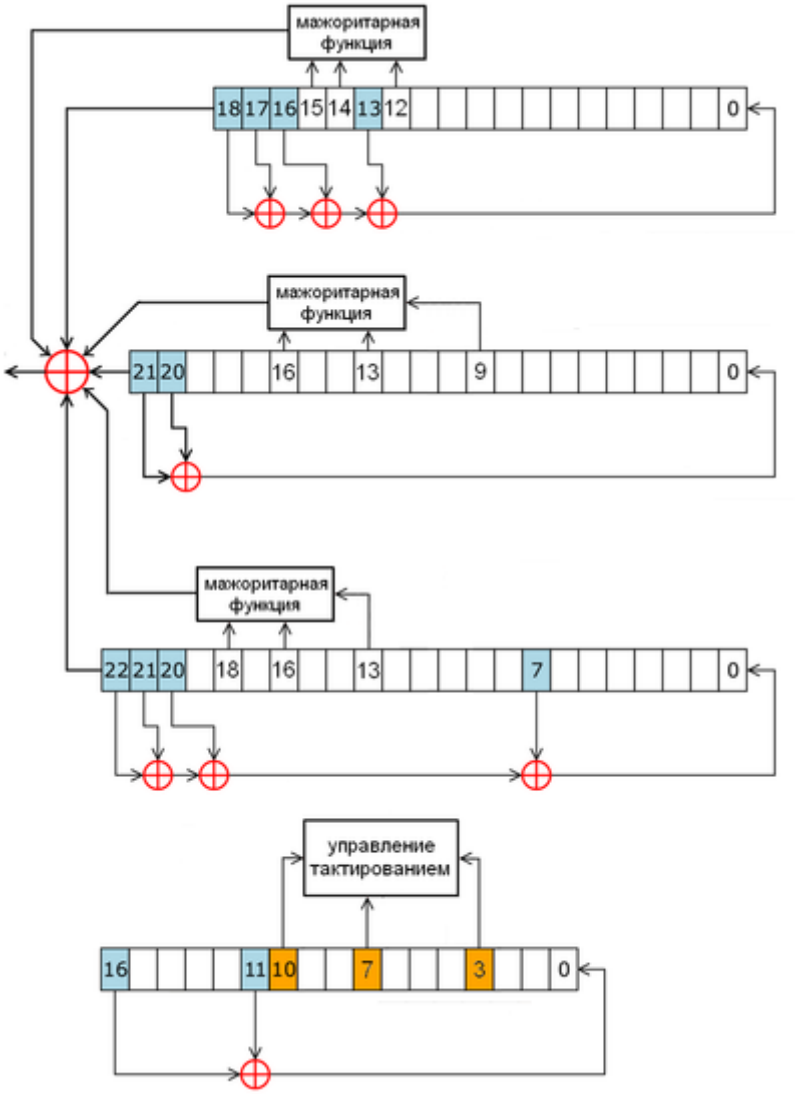
функция F = x&y|x&z|y&z,

где & — булево AND, | - булево OR, x, y и z — биты синхронизации R1, R2 и R3

- сдвигаются только те регистры, у которых бит синхронизации равен F.

Выходной бит системы — результат операции XOR над выходными битами регистров.

АЛГОРИТМ ШИФРОВАНИЯ A5/2



- добавлен регистр R4 длиной 17 бит

Многочлен обратной связи для R4:

$$X^{17} + X^{12} + 1 ,$$

Управление тактированием осуществляет R4:

биты синхронизации: 3, 7, 10

мажоритарная функция F = x&y|x&z|y&z (равна большинству), где & — булево AND, | - булево OR, а x, y и z — биты синхронизации R4(3), R4(7) и R4(10) соответственно,

R1 сдвигается если R4(10) = F
R2 сдвигается если R4(3) = F
R3 сдвигается если R4(7) = F

Выходной бит системы —XOR над старшими битами регистров и мажоритарных функций от определённых битов регистров:

R1 — 12, 14, 15,
R2 — 9, 13, 16,
R3 — 13, 16, 18.

Блок G: КОМБИНАЦИОННЫЕ ШИФРЫ

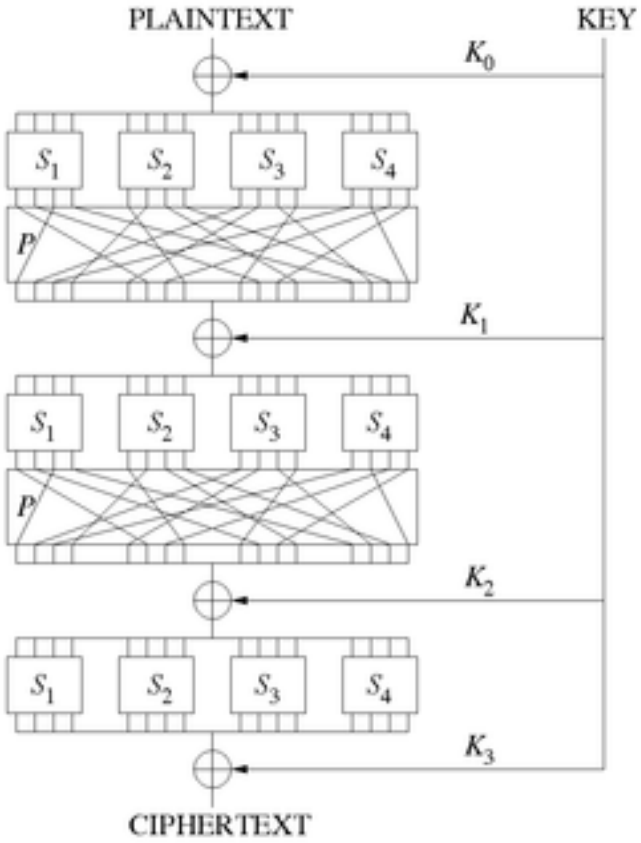
17.МАГМА
18.ГОСТ 28147-89

19.AES
20.КУЗНЕЧИК

SP-сеть.

SP-сеть (Substitution-Permutation network, **подстановочно-перестановочная сеть**) — разновидность блочного шифра, предложенная в **1971 году Хорстом Фейстелем.**

Первый тип слоя — P-слой, состоящий из P-блока большой разрядности, за ним идёт второй тип слоя — S-слой, представляющий собой большое количество S-блоков малой разрядности, потом опять P-слой и т. д.



Первым криптографическим алгоритмом на основе SP-сети была первая версия алгоритма Lucifer (1971). В следующих версиях алгоритма вместо SP-сети использовалась сеть Фейстеля, которая является альтернативой SP-сетям.

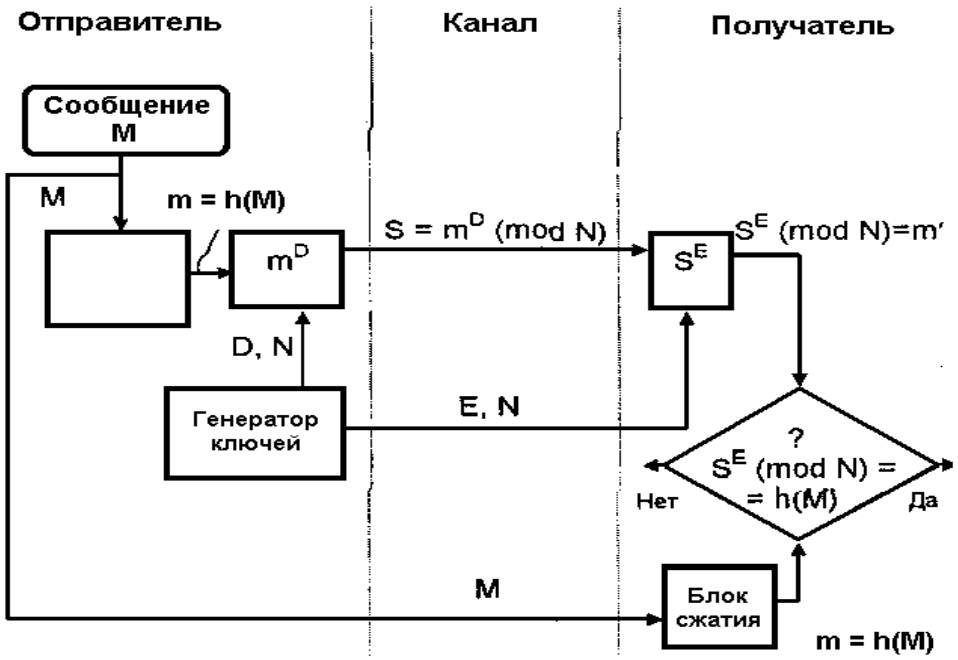
В настоящее время из алгоритмов на основе SP-сетей широко **используется AES и ГОСТ Р 34.12-2015 (Кузнечик)**.

Блок H: АЛГОРТИМЫ ЦИФРОВЫХ ПОДПИСЕЙ

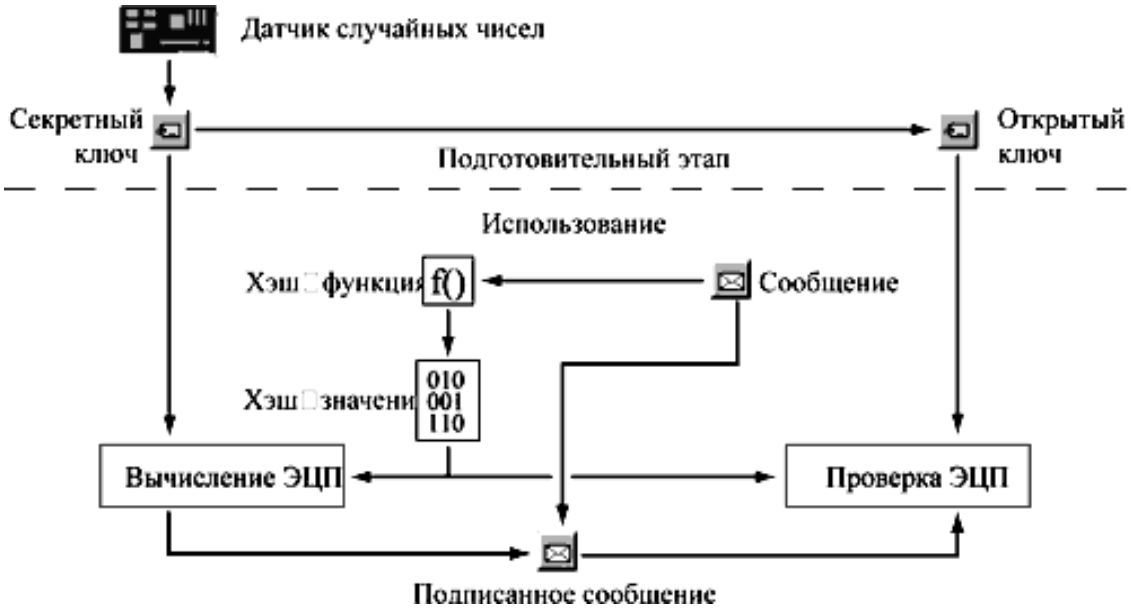
21.RSA

RSA - первый алгоритм цифровой подписи, который был разработан в 1977 году в Массачусетском технологическом институт и назван по первым буквам фамилий ее разработчиков (Ronald Rivest, Adi Shamir и Leonard Adleman). RSA основывается на сложности ***разложения большого числа n на простые множители*.**

1. **Берутся два очень больших простых числа P и Q и находятся произведение простых чисел N=P×Q и функция Эйлера от этого произведения M=(P-1)×(Q-1).**
2. **Выбирается случайное целое число D, взаимно простое с M, и вычисляется**
   E=(1 MOD M)/D.
3. **Потом D и N публикуются как открытый ключ, E сохраняется в тайне.**
4. **Если S — сообщение, длина которого, определяемая по значению выражаемого им целого числа, должна быть в интервале (1,N), то оно превращается в шифровку возведением в степень D по модулю N и отправляется получателю $S'=S^D$ MOD N.**
5. **Получатель сообщения расшифровывает его, возведя в степень E (число E ему уже известно) по модулю N, так как**
   $S=(S'^E$ MOD N)=$S(^{DE})$ MOD N.



22.El Gamal



Для того чтобы генерировать пару ключей (открытый ключ - секретный ключ), сначала выбирают некоторое **большое простое целое число P и большое целое число G, причем G < P**. Отправитель и получатель подписанного документа используют при вычислениях близкие большие целые числа **P** ($\sim 10^{308}$ или $\sim 2^{1024}$) и **G** ($\sim 10^{154}$ или $\sim 2^{512}$), которые **не являются секретными**.

1. Отправитель выбирает случайное целое число **X,**

$$1 < X \leq (P-1),$$

и вычисляет

$$Y = G^X \bmod P.$$

Y - открытый ключ.
X - секретный ключ.

2. Для того чтобы подписать сообщение M, сначала отправитель хэширует его с помощью хэш-функции h() в целое число m:

$$m = h(M),\ 1<m<(P-1),$$

и генерирует случайное целое число **К, 1 < К < (P -1**), такое, что **К и (P-1) являются взаимно простыми**.

Подписание:

отправитель вычисляет целое число **a**:

$$a = G^K \bmod P$$

и, применяя **расширенный алгоритм Евклида**, вычисляет с помощью секретного ключа X целое число **b** из уравнения

$$m = X * a + K * b \ (\text{mod}\ (P-1)).$$

Пара чисел (a,b) образует цифровую подпись S:

$$S = (a, b),$$

проставляемую под документом M.

3. (M, a, b) передается получателю.

Проверка: соответствует ли подпись S = (a, b) сообщению M.

получатель сначала вычисляет хэш по M:

$$\mathbf{m = h(M),}$$

Затем вычисляет значения

$$\mathbf{A1 = Y^a a^b \ (mod\ P)} \text{ и } \mathbf{A2 = G^m \ (mod\ P).}$$

Если **A1=A2** . т.е. $\mathbf{Y^a a^b \ (mod\ P) = G^m \ (mod\ P)}$,

подпись верна – сообщение подлинное.

23.ГОСТ Р 34.10-94

p - большое простое число длиной от 509 до 512 бит либо от 1020 до 1024 бит;
q - простой делитель числа (p -1), имеющий длину 254...256 бит;
a - любое число, большее 1 и меньшее (p-1), причем такое, что $a^q \bmod p=1$;
x - некоторое число, меньшее q;
$y = a^x \bmod p$.

Кроме того, этот алгоритм использует однонаправленную хэш-функцию H(x). Стандарт ГОСТ Р 34.11-94 определяет хэш-функцию, основанную на использовании стандартного симметричного алгоритма ГОСТ 28147-89.

Первые три параметра **p, q и a являются открытыми** и могут быть общими для всех пользователей сети. Число **x** является секретным ключом. Число **y** является открытым ключом. Чтобы подписать некоторое сообщение **m**, а затем проверить подпись, выполняются следующие шаги.

1. Пользователь A генерирует случайное число k, причем k<q.
2. Пользователь A вычисляет значения

   $r = (a^k \bmod p) \bmod q$,

   $s = (x * r + k\,(H(m))) \bmod q$.

   Если $H(m) \bmod q=0$, то значение $H(m) \bmod q$ принимают равным единице.

   Если r=0, то выбирают другое значение k и начинают снова.

   Цифровая подпись представляет собой два числа:

   $r \bmod 2^{256}$ и $s \bmod 2^{256}$

   Пользователь A отправляет эти числа пользователю B.
3. Пользователь B проверяет полученную подпись, вычисляя

   $v = H(m)^{q-2} \bmod q$,

   $z_1 = (s * v) \bmod q$,

   $z_2 = ((q-r) * v) \bmod q$,

   $u = ((a^{z1} * y^{z2}) \bmod p) \bmod q$.

   Если u = r, то подпись считается верной.

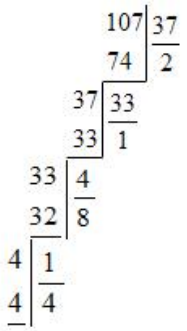
П р и м е р. Решим сравнение

$$111x = 75 \pmod{321}. \qquad (4)$$

Здесь (111, 321) = 3, причем 75 кратно 3. Поэтому сравнение имеет три решения. Деля обе части сравнения и модуль на 3, получим сравнение

$$37x = 25 \pmod{107}, \qquad (5)$$

которое нам следует сначала решить. Имеем



n		1	2	3	4
q		2	1	8	4
P_n	1	2	3	26	107

Значит, в данном случае $n = 4$, $P_{n-1} = 26$, $b = 25$, и мы имеем решение сравнения (5) в виде

$$x \equiv -26 \cdot 25 \equiv 99 \pmod{107}.$$

Отсюда решения сравнения (4) представляются так:

$$x \equiv 99;\ 99 + 107;\ 99 + 2 \cdot 107 \pmod{321},$$

т. е.

$$x = 99;\ 206;\ 313 \pmod{321}.$$

24.ГОСТ Р 34.10-2012

Таблица 4

Основные соотношения для старого и нового стандартов ЭЦП

Алгоритм	ГОСТ Р34.10–94 (старый)	ГОСТ Р34.10–01 (новый)
Выработка ключевой пары	p – простое число, $509 \leqslant \lvert p \rvert \leqslant 512$ или $1020 \leqslant \lvert p \rvert \leqslant 1024$, q – простое число, делитель (p-1), $254 \leqslant \lvert q \rvert \leqslant 256$, a – любое натуральное число, такое, что $1<a<p-1, a^q=1 \bmod p$, x – любое число: $0<x<q$ $y=a^x \bmod p$	p – простое число, $p>2^{255}$, E – эллипт. кривая над GF(p), q – простое число, делитель порядка группы точек E, $2^{254} < q < 2^{256}$ $P \in E$ – любая точка кривой, такая, что $P \neq O, qP = O$; x – любое число: $0<x<q$, $Q=xP$
Ключи	Общий открытый ключ сети: (p, q, a). Открытый ключ пользователя: y. Секретный ключ пользователя: x	Общий открытый ключ сети: (p, E, P). Открытый ключ пользователя: Q. Секретный ключ пользователя: x
Подпись	Генерируется случайное число $0<k<q$, $r=(a^k \bmod p) \bmod q$, $s=(xr+kH) \bmod q$. Подпись: (r, s).	Генерируется случайное число $0<k<q$, $C = kP$, $r=x_c \bmod q$, $s=(xr+kH) \bmod q$. Подпись: (r, s).
Проверка подписи	$v=H^{q-2} \bmod q$, $z=sv \bmod q$, $w=(q-r)v \bmod q$, $u=(a^z y^w \bmod p) \bmod q$. Подпись верна, если u=r	$v=H^{-1} \bmod q$, $z=sv \bmod q$, $w=(q-r)v \bmod q$, $C = zP + wQ$, $u=x_c \bmod q$. Подпись верна, если u=r

Операция умножения точки на некоторое число **k** (на скаляр) называется ***композицией точки на эллиптической кривой*** и является аналогом операции возведения в степень k.

Операцию **умножения точки на число** можно представить, как процесс сложения точки самой с собой нужное число раз.

Например:

$$2P = P + P,$$
$$3P = 2P + P$$

и т.д.

Существует способ быстрого умножения точки на число, который требует $O(\log k \log^3 p)$ количества операций для умножения точки $P \in E$, определенной в конечном поле F_p на некоторое число k. Этот метод аналогичен алгоритму быстрого возведения в степень для элементов конечного поля, действительно:

$$100P = 2(2(P + 2(2(2(P + 2P))))).$$

Операции сложения и удвоения точек имеют аналитические выражения.

Сложение точек:

Пусть $P(x_1, y_1), Q(x_2, y_2) \in E$ – две точки, для которых $x_1 \neq x_2$. Тогда $P + Q = R(x_3, y_3)$, где

$$x_3 = \lambda^2 - x_1 - x_2,$$
$$y_3 = \lambda(x_1 - x_3) - y_1,$$

и

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}.$$

Удвоение точки:

Пусть точка $P(x_1, y_1) \in E$, для которой $y_1 \neq 0$ (если $y_1 = 0$, тогда $P = -P$, т.е. $2P = O$), тогда $2P = (x_3, y_3)$, где

$$x_3 = \lambda^2 - 2x_1,$$
$$y_3 = \lambda(x_1 - x_3) - y_1,$$

где

$$\lambda = \frac{3x_1^2 + a}{2y_1}.$$

БЛОК J: ОБМЕН КЛЮЧАМИ

25.ОБМЕН КЛЮЧАМИ ПО ДИФФИ-ХЕЛЛМАНУ

В протоколе обмена секретными ключами предполагается, что все пользователи знают некоторые числа **n** и **a** (1< a < n). Для выработки общего секретного ключа пользователи А и В должны проделать следующую процедуру:

1. Определить секретные ключи пользователей $К_A$ и $К_B$.

Для этого каждый пользователь независимо выбирает случайные числа из интервала (2,..., n-1).

2. Вычислить открытые ключи пользователей Y_A и Y_B.

Для этого каждый использует одностороннюю показательную функцию

$$Y=a^K \bmod n$$ со своим секретным ключом.

3. Обменяться ключами Y_A и Y_B по открытому каналу связи.
4. Независимо определить общий секретный ключ К:

$$K=Y^K \bmod n$$

(пользователи выполняют вычисления с помощью той же односторонней функции).

Доказательство:

A: $Y_B^{KA} (\bmod n) = [a^{KB}]^{KA} \bmod n = a^{KA*KB} \bmod n = K.$

B: $Y_A^{KB} (\bmod n) = [a^{KA}]^{KB} \bmod n = a^{KB*KA} \bmod n = K.$

СТАНДАРТЫ

1. ГОСТ 28147-89
2. ГОСТ Р 34.10-2012
3. ГОСТ Р 34.11-2012
4. ГОСТ Р 34.12-2015
5. ГОСТ Р 34.13-2015

ВОПРОСЫ К ЗАЧЕТУ

1. Какая конструкция лежит в основе алгоритма Магма? Блок-схема.
2. Какая конструкция лежит в основе алгоритма Кузнечик? Блок-схема.
3. Что общего и чем отличаются криптосистемы Магма и Кузнечик?
4. Какие требования к ключевой системе регламентированы ГОСТ 28147-89?
5. Какие требования к ключевой системе регламентированы ГОСТ Р 34.10-2012?

6. Какие требования к ключевой системе регламентированы ГОСТ Р 34.12-2015?
7. Какой алгоритм лежит в основе ГОСТ Р 34.10-2012?
8. Как происходит проверка цифровой подписи в ГОСТ Р 34.10-2012?
9. В процессе формирования цифровой подписи сначала производится хеширование или шифрование? Зачем?
10. На каком ключе, открытом или секретном, производится шифрование в ГОСТ Р 34.10? Проверка ЦП?
11. Для чего в ГОСТ Р 34.10-2012 предусмотрен выбор длины ЦП?
12. Какова длина ЦП по ГОСТ Р 34.10-2012?
13. На чем основана криптостойкость ГОСТ Р 34.10-2012? ГОСТ Р 34.12-2015?
14. Какие требования к хеш-функциям сформированы в ГОСТ Р 34.11-2012?
15. С помощью каких процедур формируется значение хеш-функции?
16. Сколько и какие режимы шифрования специфицирует ГОСТ Р 34.13-2015?
17. Как влияет выбор режима шифрования на криптостойкость криптосистемы ГОСТ Р 34.12-2015?
18. По каким критериям выбирается режим шифрования?
19. Назовите области применения криптографии в гражданской практике (не менее 10).

ВОПРОСЫ К ЭКЗАМЕНУ

1. Нарисовать блок схему алгоритма шифра Вернама.
2. Привести числовой пример с линейным генератором гаммы с максимальным периодом.
3. Нарисовать блок-схему алгоритма обмена ключами по схеме Диффи-Хеллмана.
4. Нарисовать блок-схему алгоритма шифра RSA.
5. Нарисовать блок-схему алгоритма шифра Эль-Гамаля.
6. Нарисовать блок-схему цифровой подписи по алгоритму RSA.
7. Нарисовать блок-схему алгоритма криптографической хеш-функции.
8. Нарисовать блок-схему цифровой подписи по алгоритму EGSA.
9. Нарисовать блок-схему алгоритма шифрования данных Эль-Гамаля.
10. Нарисовать блок-схему генерации частного открытого ключа по алгоритму ГОСТ Р 34.10-2012.
11. Нарисовать блок-схему генерации гаммы по стандарту ГОСТ Р 34.12-2015.
12. Нарисовать блок-схему расшифрования данных по алгоритму Эль-Гамаля.
13. Нарисовать блок-схему цифровой подписи по алгоритму ECDSA.
14. Нарисовать блок-схему проверки цифровой подписи по алгоритму DSA.
15. Нарисовать блок-схему алгоритма сложения двух точек эллиптической кривой над конечным полем.
16. Нарисовать блок-схему алгоритма удвоения точки эллиптической кривой над конечным полем.
17. Нарисовать блок-схему цифровой подписи по алгоритму ГОСТ Р 34.10-94.
18. Нарисовать блок-схему цифровой подписи по алгоритму ГОСТ Р 34.10-2012.
19. Нарисовать блок-схему функции шифрования данных по стандарту ГОСТ Р 34.12-2015.
20. Нарисовать блок-схему функции шифрования данных по стандарту DES.
21. Нарисовать блок-схему алгоритма замены по таблице ГОСТ Р 34.12-2015.
22. Нарисовать блок-схему шифрования данных по стандарту ГОСТ Р 34.12-2015 (МАГМА).
23. Нарисовать блок-схему шифрования данных по стандарту ГОСТ Р 34.12-2015 (Кузнечик).
24. Нарисовать блок-схему шифрования данных по стандарту DES.
25. Нарисовать блок-схему шифрования данных по стандарту AES.
26. Привести числовой пример.