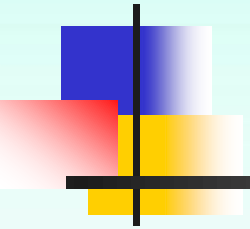
CRYPTOGRAPHY



МЕТОДИ ТА ЗАСОБИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Лек. 12 2022 КІБ-19

АБСТРАКТНАЯ АЛГЕБРА

ПОЛЯ ГАЛУА

Алгебраические структуры

Алгебраическая структура	Операции	Наборы целых
Группа	$(+ \ -)$ или $(\times \ \div)$	$\mathbb{Z}_n$ или $\mathbb{Z}_n^*$
Кольцо	$(+ \ -)$ и $(\times)$	$\mathbb{Z}$
Поле	$(+ \ -)$ и $(\times \ \div)$	$\mathbb{Z}_p$

ПОЛЕ - суть множество, в котором можно **складывать, вычитать, умножать и делить**!

Поле Галуа $GF(p^n)$

Поле Галуа $GF(p^n)$ это конечное поле с p^n элементами, где p - простое число (характеристика поля), n - целое ≥ 1 (степень поля).

Если $n = 1$, то поле Галуа $\rightarrow$ $GF(p)$ - конечное поле с p элементами. То есть множество S суть $\mathbb{Z}_p$.
Если $p = 2$, то поле Галуа $\rightarrow$ $GF(2^n) \rightarrow$ элементы поля можно задавать как n-битовые слова.

Эвари́ст Галуа́ (1811- 1832, Франция) — французский математик, основатель современной высшей алгебры.

Поле Галуа $GF(2)$

Поле Галуа $GF(2^1)$ это конечное поле с 2 элементами и двумя операциями $\oplus$,$\otimes$

!!! $\mathbb{Z}_p$, **булева** алгебра.
Элементы поля: объекты T и F или биты 0,1.

Операция $\oplus$- СЛОЖЕНИЕ → **XOR.**
Операция $\otimes$- УМНОЖЕНИЕ → **AND.**
Сложение и аддитивная инверсия (вычитание) операция **XOR.**
Умножение и мультипликативная инверсия (деление) операция **AND.**

Поле Галуа $GF(2)$

$GF(2)$ – булева алгебра - конечное поле с 2 элементами $0, 1$ и операциями $\oplus, \otimes$

$\oplus$

	0	1
0	0	1
1	1	0

$\otimes$

	0	1
0	0	0
1	0	1

Инверсия $\oplus$

A	0	1
-A	1	0

Инверсия $\otimes$

A	0	1
-A	-	1

Поле Галуа $GF(5)$

Поле Галуа $GF(5)$ это конечное поле с 5 элементами $0, 1, 2, 3, 4$ и операциями $\oplus, \otimes$

$\oplus$

	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\otimes$

	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Инверсия $\oplus$

A	0	1	2	3	4
-A	0	4	3	2	1

Инверсия $\otimes$

A	0	1	2	3	4
A^{-1}	-	1	3	2	4

Поле Галуа $GF(2^2)$

Поле Галуа $GF(2^2)$ это конечное поле с 4 элементами. Определим элементы поля как $00, 01, 10, 11$ и операции $\oplus, \otimes$ как:

$\oplus$

	00	01	10	11
00	00	01	10	11
01	01	00	11	10
10	10	11	00	01
11	11	10	01	00

$\otimes$

	00	01	10	11
00	00	00	00	00
01	00	01	10	11
10	00	10	11	01
11	00	11	01	10

Инверсия $\oplus$

A	00	01	10	11
-A	00	01	10	11

Инверсия $\otimes$

A	00	01	10	11
A^{-1}	-	01	11	10

Поле Галуа $GF(2^n)$

Поле Галуа $GF(2^n)$ это конечное поле с 2^n элементами - n-битовыми словами.
Пусть: $n = 4 \rightarrow GF(16)$

$$S = \begin{Bmatrix} 0000, 0001, 0010, 0011, \\ 0100, 0101, 0110, 0111, \\ 1000, 1001, 1010, 1011, \\ 1100, 1101, 1110, 1111 \end{Bmatrix}$$

!!! 16 – не простое → для поля надо выписать таблицу умножения, так, что бы для каждого элемента S была мультипликативная инверсия!!!

Поле Галуа $GF(2^n)$ и Многочлены (полиномы) над полем

Полином $f(x)$ над полем $GF(2^n)$ имеет вид

$$f(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots a_1x^1 + a_0x^0$$

$$a_i \in GF(2), \qquad a_i = \{0, 1\}$$

Здесь:

x – формальная переменная ,

$\deg(f(x)) = n - 1$ - целое неотрицательное число – степень полинома $f(x)$.

Полином можно задавать просто как кортеж коэффициентов из $GF(2)$.

Поле Галуа $GF(2^n)$ и Многочлены (полиномы) над полем

Полином $f(x)$ можно представить в виде

$$f(x) = \sum_{i=0}^{n-1} a_i x^i, a_i \in GF(2)$$

!! Умножение задается правилами
$x^k * x^m = x^{k+m}$, $x^0 \equiv 1$.
Полином нормирован → $a_{n-1} = 1$.
Сумма и произведение полиномов выполняются обычным образом, **НО** операции с коэффициентами в поле $GF(2)$.

Поле Галуа $GF(2^n)$ и Многочлены (полиномы) над полем

Например: $p = 2, n = 3 \rightarrow GF(2^3)$.

Элементы множества 000, 001, …, 111 можно задать как множество полиномов:

000	$0x^2 + 0x^1 + 0x^0 = 0$
001	$0x^2 + 0x^1 + 1x^0 = 1$
010	$0x^2 + 1x^1 + 0x^0 = x$
011	$0x^2 + 1x^1 + 1x^0 = x + 1$
100	$1x^2 + 0x^1 + 0x^0 = x^2$
101	$1x^2 + 0x^1 + 1x^0 = x^2 + 1$
110	$1x^2 + 1x^1 + 0x^0 = x^2 + x$
111	$1x^2 + 1x^1 + 1x^0 = x^2 + x + 1$

Поле Галуа $GF(2^n)$ и Многочлены (полиномы) над полем

Например: $p = 2, n = 4 \rightarrow GF(2^4)$.

Элементы множества 0000, 0001, …, 1111 можно задать как множество полиномов:

0000	$0x^3 + 0x^2 + 0x^1 + 0x^0$	1000	$1x^3 + 0x^2 + 0x^1 + 0x^0$
0001	$0x^3 + 0x^2 + 0x^1 + 1x^0$	1001	$1x^3 + 0x^2 + 0x^1 + 1x^0$
0010	$0x^3 + 0x^2 + 1x^1 + 0x^0$	1010	$1x^3 + 0x^2 + 1x^1 + 0x^0$
0011	$0x^3 + 0x^2 + 1x^1 + 1x^0$	1011	$1x^3 + 0x^2 + 1x^1 + 1x^0$
0100	$0x^3 + 1x^2 + 0x^1 + 0x^0$	1100	$1x^3 + 1x^2 + 0x^1 + 0x^0$
0101	$0x^3 + 1x^2 + 0x^1 + 1x^0$	1101	$1x^3 + 1x^2 + 0x^1 + 1x^0$
0110	$0x^3 + 1x^2 + 1x^1 + 0x^0$	1110	$1x^3 + 1x^2 + 1x^1 + 0x^0$
0111	$0x^3 + 1x^2 + 1x^1 + 1x^0$	1111	$1x^3 + 1x^2 + 1x^1 + 1x^0$

Поле Галуа $GF(2^n)$ и Многочлены (полиномы) над полем

Пример: $n = 8, 2^n = 256$ – элементов

Элемент множества 00100110

Его полиномиальное представление $f(x) = 0x^7 + 0x^6 + 1x^5 + 0x^4 + 0x^3 + 1x^2 + 1x^1 + 0x^0 =$

$$x^5 + x^2 + x$$

Поле Галуа $GF(2^n)$ и полиномы

Обычные операции, коэффициенты в $\mathbb{Z}_q$

Сложение полиномов.

Заданы $f(x) = \sum_{i=0}^{n-1} a_i\, x^i, \quad g(x) = \sum_{i=0}^{n-1} b_i\, x^i,$

То $f(x) + g(x) = \sum_{i=0}^{n-1} (a_i + b_i) x^i.$

!!!if$(a_i + b_i) > q \rightarrow \deg\big(f(x) \times g(x)\big) = n$

Умножение полиномов.

Заданы $f(x) = \sum_{i=0}^{n-1} a_i\, x^i, \quad g(x) = \sum_{j=0}^{n-1} b_j\, x^j,$

Тогда $s(x) = f(x) \times g(x) = \sum_{k=0}^{2n} s_k\, x^k$

и $s_k = \sum_{k=i+j} a_i b_i$. !!! $\deg\big(f(x) \times g(x)\big) = 2n$

В $GF(2^n)$ нет таких элементов !! МОДУЛЬ !!

Поле Галуа $GF(2^n)$ и Факторизация полиномов

Факторизация полинома – представление полинома в виде произведения полиномов меньшей степени

Полином $f(x)$ представляется в виде

$$f(x) = h(x) \times g(x)$$

Причем $\deg\big(h(x) \times g(x)\big) = \deg\big(f(x)\big)$

Канонически: $f(x) = x^3 + x^2 + x + 1 =$

$$(x + \alpha)\ (x + \delta)\ (x + \gamma)$$

Поле Галуа $GF(2^n)$ и полиномы

Операции

Операция деления (делимость).

Заданы $f(x) = \sum_{i=0}^{n-1} a_i\, x^i, \quad g(x) = \sum_{j=0}^{m-1} b_j\, x^j,$
Пусть $g(x) \neq 0$ **– не тождественный нуль.**
Полином $f(x)$ **делится на** $g(x)$ **если есть такой полином** $h(x)$ **, что** $f(x) = g(x) \times h(x)$.
ЕСТЬ !!! Записывается как $g(x) | f(x)$
НЕТ !!! Записывается как $g(x) \nmid f(x)$
$g(x)$**- делитель (сомножитель) полинома** $f(x)$

$$\deg(g(x)) \leq \deg(f(x))$$

Существует $gcd(f(x), h(x))$.
!!! Аналог алгоритма Эвклида!

Поле Галуа $GF(2^n)$ и полиномы

Обратимый полином

«Аналог обратного числа»

Для полиномов:

Полином $f(x) \in GF(2^n)$ называется обратимым если в $GF(2^n)$ найдется такой полином $g(x)$, что

$$f(x) \times g(x) = 1 .$$

Иначе $f(x)$ необратим .

Если обратим то

$$g(x) = f(x)^{-1} .$$

Поле Галуа $GF(2^n)$ и полиномы

Неприводимый полином

«Аналог простого числа»

Для полиномов:

Полином $p(x) \in GF(2^n)$ **называется неприводимым если в любом разложении**

$$p(x) = g(x) \times h(x)$$

или $\deg(g(x)) = 0$**, или** $\deg(h(x)) = 0$**.**

Поле Галуа $GF(2^n)$ и полиномы
Неприводимые полиномы над GF(2)

№	Deg(f)	Полином
1	1	$x+1$
2	2	x^2+x+1
3	3	x^3+x+1
4	3	x^3+x^2+1
5	4	x^4+x+1
6	4	x^4+x^2+1

№	Deg(f)	Полином
7	5	x^5+x+1
8	5	x^5+x^3+1
9	5	$x^5+x^3+x^2+x+1$
10	5	$x^5+x^4+x^2+x+1$
11	5	$x^5+x^4+x^3+x+1$
12	5	$x^5+x^4+x^3+x^2+1$

№	Deg(f)	Полином
40	8	$x^8+x^4+x^3+x+1$
41	8	$x^8+x^4+x^3+x^2+1$
……	…….	……
68	8	$x^8+x^7+x^6+x^5+x^4+x^2+1$
69	8	$x^8+x^7+x^6+x^5+x^4+x^3+1$

Арифметика Поля Галуа $GF(2^n = 2^3)$

Сложение / вычитание

$$f(x) = \sum_{i=0} (a_i \oplus b_i) x^i$$

	000	001	010	011	100	101	110	111
000	000	001	010	011	100	101	110	111
001	001	000	011	010	101	100	111	110
010	010	011	000	101	110	111	100	101
011	011	010	001	000	111	110	101	100
100	100	101	110	111	000	001	010	011
101	101	100	111	110	001	000	011	010
110	110	111	100	101	010	011	000	001
111	111	110	101	100	011	010	001	000

Арифметика Поля Галуа $GF(2^n = 2^8)$

Сложение / вычитание

Заданы $g(x) = \sum_{i=0}^{7} a_i x^i$, $h(x) = \sum_{i=0}^{7} b_i x^i$,

То $f(x) = g(x) + h(x) = \sum_{i=0}^{7}(a_i + b_i)x^i$

$a_i, b_i = \{0, 1\}$, то есть сложение в коэффициентов в поле $GF(2)$ и, следовательно

$$f(x) = \sum_{i=0}(a_i \oplus b_i)x^i$$

Аддитивный нейтральный элемент – нулевой полином.

Аддитивная инверсия полинома – сам полином.

Арифметика Поля Галуа $GF(2^n = 2^8)$
Сложение / вычитание

Пример
Заданы:

$$g(x) = x^5 + x^2 + x =$$
$$0x^7 + 0x^6 + 1x^5 + 0x^4 + 0x^3 + 1x^2 + 1x^1 + 0x^0$$

$$h(x) = x^3 + x^2 + 1 =$$
$$0x^7 + 0x^6 + 0x^5 + 0x^4 + 1x^3 + 1x^2 + 0x^1 + 1x^0.$$

Суммируем по модулю 2 коэффициенты и получаем

$$0x^7 + 0x^6 + 1x^5 + 0x^4 + 1x^3 + 0x^2 + 1x^1 + 1x^0$$

Т.е. $f(x) = x^5 + x^3 + x + 1$

Арифметика Поля Галуа $GF(2^n = 2^3)$

Умножение

$$f(x) = g(x) \times h(x) = (g(x) * h(x)) mod\ p(x)$$

$p(x)$ - неприводимый полином в $GF(2^3)$

	000	001	010	011	100	101	110	111
000	000	000	000	000	000	000	000	000
001	000	001	010	011	100	101	110	111
010	000	010	100	110	101	111	001	011
011	000	011	110	101	001	010	111	100
100	000	100	101	001	111	011	010	110
101	000	101	111	010	011	110	100	001
110	000	110	001	111	010	100	011	101
111	000	111	011	100	110	001	101	010

$$p(x) = x^3 + x^2 + 1 = 1101$$

Арифметика Поля Галуа $GF(2^n = 2^4)$

Умножение

Заданы $g(x) = \sum_{i=0}^{3} a_i\, x^i, \quad h(x) = \sum_{i=0}^{3} b_i\, x^i,$

То

$$f(x) = g(x) \times h(x) = \big(g(x) * h(x)\big) mod\, p(x)$$

$p(x)$ **- неприводимый полином в** $GF(2^4)$

Причем:

- **умножение коэффициентов в поле** $GF(2)$ **, т.е по модулю 2**
- **умножение** x^i **на** x^j **дает** x^{i+j}
- **каноническое произведение берется по модулю** $p(x)$**.**

Арифметика Поля Галуа $GF(2^n = 2^8)$
Умножение

Пример. Заданы:

$$g(x) = x^5 + x^2 + x =$$
$$0x^7 + 0x^6 + 1x^5 + 0x^4 + 0x^3 + 1x^2 + 1x^1 + 0x^0$$
$$h(x) = x^7 + x^4 + x^3 + x^2 + x =$$
$$1x^7 + 0x^6 + 0x^5 + 1x^4 + 1x^3 + 1x^2 + 1x^1 + 0x^0.$$
$$f(x) = x^5 * (x^7 + x^4 + x^3 + x^2 + x) +$$
$$x^2 * (x^7 + x^4 + x^3 + x^2 + x) +$$
$$x * (x^7 + x^4 + x^3 + x^2 + x)$$

$$f(x) = x^5x^7 + x^5x^4 + x^5x^3 + x^5x^2 + x^5x^1 + x^2x^7 + x^2x^4 + x^2x^3 + x^2x^2$$
$$+ x^2x^1 + x^1x^7 + x^1x^4 + x^1x^3 + x^1x^2 + x^1x^1 =$$
$$x^{12} + x^9 + x^8 + x^7 + x^6 + x^9 + x^6 + x^5 + x^4 + x^3 + x^8 + x^5 + x^4 + x^3 + x^2$$
$$= x^{12} + x^7 + x^2$$

Арифметика Поля Галуа $GF(2^n = 2^8)$
Умножение

Пример. Продолжение:

Полином модуль

$$p(x) = x^8 + x^4 + x^3 + x + 1$$

Делим $x^{12}+x^7+x^2$ **на** $x^8 + x^4 + x^3 + x + 1$

$x^{12} + x^7 + x^2$ | $x^8 + x^4 + x^3 + x + 1$

$x^{12} + x^8 + x^7 + x^5 + x^4$ | $x^4 + 1$

$x^8 + x^5 + x^4 + x^2$

$x^8 + x^4 + x^3 + x + 1$

$x^5 + x^3 + x^2 + x + 1$

Мультипликативный нейтральный элемент – мультипликативная единица всегда 1.

Арифметика Поля Галуа $GF(2^n = 2^8)$

Мультипликативная инверсия

Мультипликативная инверсия ищется с помощью расширенного алгоритма Эвклида. Алгоритм применяется к искомому полиному и модулю-полиному.

!!!! Все операции с коэффициентами в поле $GF(2)$. Сложение, умножение - по вышеприведенным правилам

Арифметика Поля Галуа $GF(2^n = 2^8)$

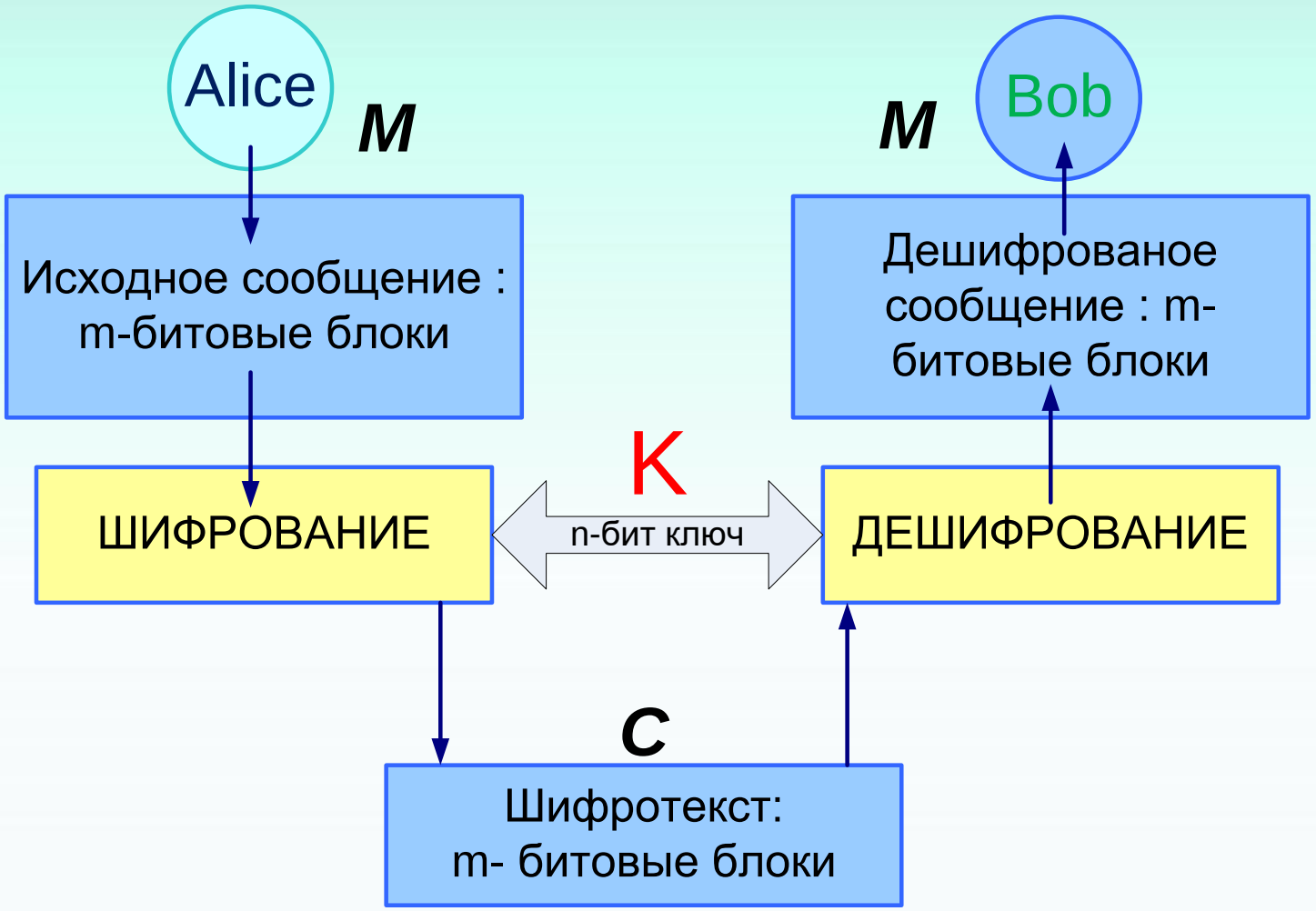
Мультипликативная инверсия

Пример: Найти мультипликативную инверсию $f(x) = x^5$ по модулю $p(x) = x^8 + x^4 + x^3 + x + 1$.

r1	r2	r	q	t1	t2	t
$x^8 + x^4 + x^3 + x + 1$	x^5	$x^4 + x^3 + x + 1$	x^3	0	1	x^3
x^5	$x^4 + x^3 + x + 1$	$x^3 + x^2 + 1$	$x + 1$	1	x^3	$x^4 + x^3 + 1$
$x^4 + x^3 + x + 1$	$x^3 + x^2 + 1$	1	x	x^3	$x^4 + x^3 + 1$	$x^5 + x^4 + x^2 + x$
$x^3 + x^2 + 1$	1	0	1	$x^4 + x^3 + 1$	$x^5 + x^4 + x^2 + x$	0
1	0		0	$x^5 + x^4 + x^2 + x$	0	

$$x^{5^{-1}} mod\ (x^8 + x^4 + x^3 + x + 1) = x^5 + x^4 + x^2 + x\ .$$

Блочные шифры с симметричным ключом в $GF(2^n)$



Современные блочные шифры
С симметричным ключом

!!! Проектируется как шифр подстановки

Но все в поле Галуа $GF(2^n)$

Современные блочные шифры
С симметричным ключом

Пример «мультипликативный шифр»

$$M = \{s|\ s \in GF(2^n)\}, \qquad C = \{c|\ c \in GF(2^n)\},$$

$$K = \{k|\ k \in GF(2^n)^{>0}\ \}$$

$$E(M) = (s * k)(mod\ p)$$

Ключи шифрования / дешифрования должны быть мультипликативно инверсны в $GF(2^n)$ ***!!!***

$$D(C) = \left(c * k^{-1}\right)(mod\ p)$$

Современные блочные шифры
С симметричным ключом

Пример «одноразовый блокнот→электронная кодовая книга»

Случайным образом задается вектор $\boldsymbol{K}$ ключей с количеством элементов равным длине сообщения – $\boldsymbol{k_i \in GF(2^n)}$!

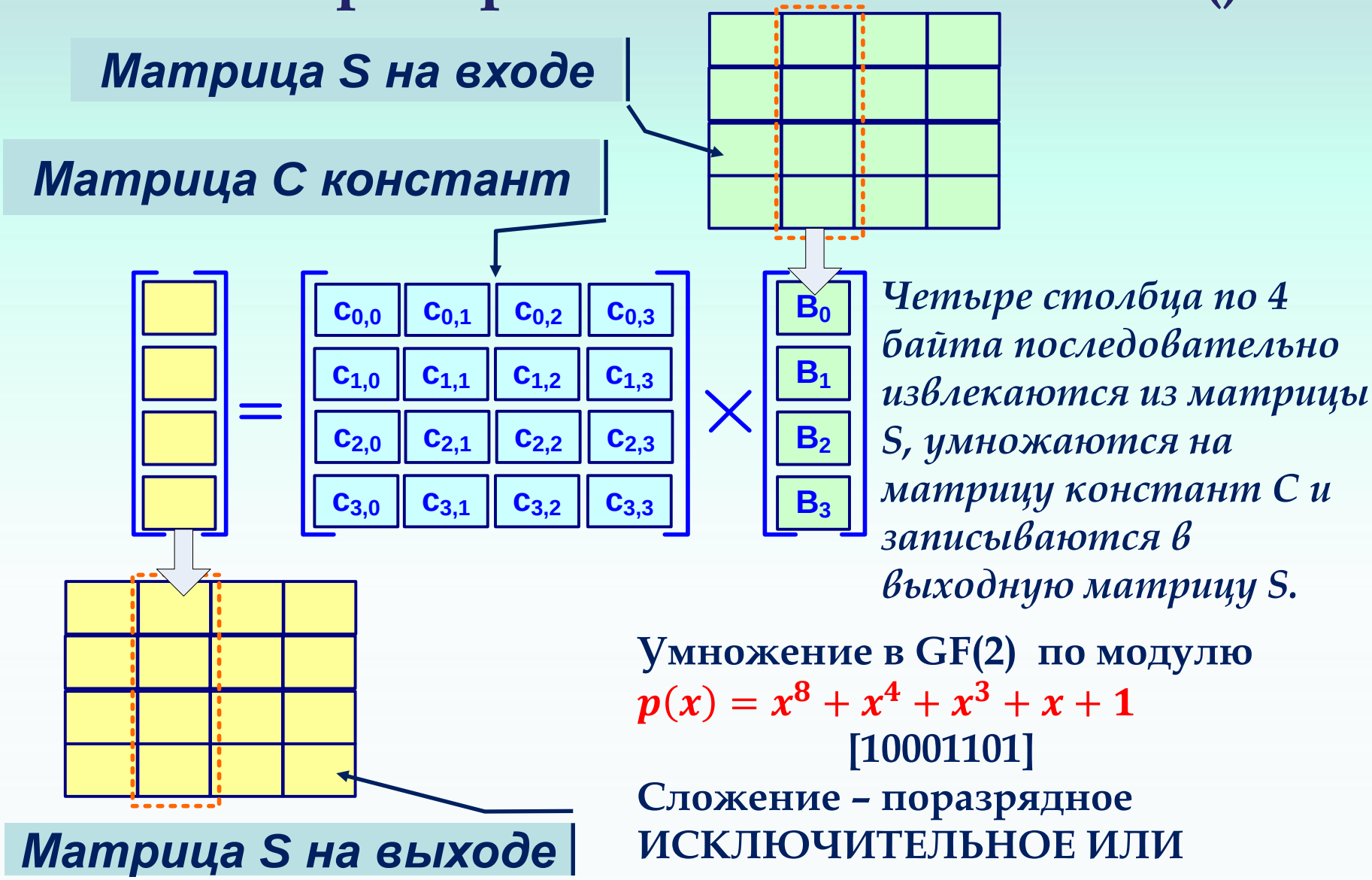
$$\boldsymbol{K} = \begin{bmatrix} \boldsymbol{k_0} \\ \boldsymbol{k_i} \\ \boldsymbol{k_L} \end{bmatrix}$$

$$\boldsymbol{k_t = k_i}$$

$\boldsymbol{c_t = (s_t + k_t)}$ или $\boldsymbol{c_t = (s_t \times k_t)\ mod\ p}$

$\boldsymbol{c_t = (s_t + k_t)}$ или $\boldsymbol{m_t = \left(c_t \times k^{-1}{}_t\right) mod\ p}$

AES преобразование MixColumns()



Четыре столбца по 4 байта последовательно извлекаются из матрицы S, умножаются на матрицу констант C и записываются в выходную матрицу S.

Умножение в GF(2) по модулю

$$p(x) = x^8 + x^4 + x^3 + x + 1$$

[10001101]

Сложение – поразрядное ИСКЛЮЧИТЕЛЬНОЕ ИЛИ

AES преобразование MixColumns()

Direct C

02	03	01	01
01	02	03	01
01	01	02	03
01	01	01	02

Invers C

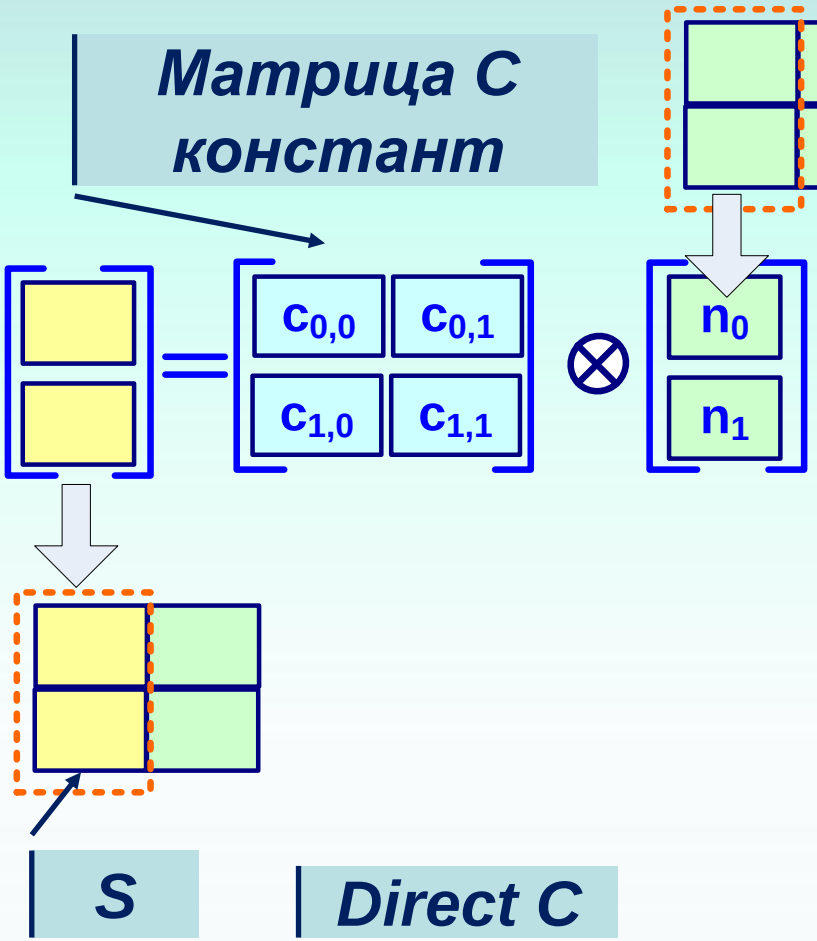
0E	0B	0D	09
09	0E	0B	0C
0D	09	0E	0B
0B	0D	09	0E

Например, первый байт результата (строка X столбец)

$$b_0 = (02 \odot S_{0,c}) \oplus (03 \odot S_{1,c}) \oplus S_{2,c} \oplus S_{3,c}$$

MixColumns() ← → InvMixColumns()

S-AES MixColumns



Умножение в GF(2) по модулю [10011]
Сложение – поразрядное ИСКЛЮЧИТЕЛЬНОЕ ИЛИ

Direct C

1	4
4	1

Invers C

9	2
2	9

S-AES MixColumns

Sout[0][0] = Con[0][0] ⊙ Sin[0][0] ⊕ Con[0][1] ⊙ Sin[1][0]
Sout[1][0] = Con[1][0] ⊙ Sin[0][0] ⊕ Con[1][1] ⊙ Sin[1][0]

Sout[0][0] = Sin[0][0] ⊕ [0 1 0 0] ⊙ Sin[1][0]
Sout[1][0] = [0 1 0 0] ⊙ Sin[0][0] ⊕ Con[1][1]

Sout[0][0] = Sin[0][0] ⊕ ([0 1 0 0] X Sin[1][0]) mod[10011]
Sout[1][0] = ([0 1 0 0] X Sin[0][0]) mod[10011] ⊕ Con[1][1]

Например:

Sin[0][0] = [0 1 1 0] ; Sin[1][0]) = [1 1 0 1]
[0 1 0 0] X [1 1 0 1] = [1 1 0 1 0 0]
[1 1 0 1 0 0] mod [1 0 0 1 1]
В полиномиальном виде
делим $f(x) = x^5+x^4+x^2$ **на** $p(x) = x^4 + x + 1$

S-AES MixColumns

$x^5 + x^4 + + x^2 + + \quad \Big| \quad x^4 + x + 1$

$x^5 + + + x^2 + x \quad \Big| \quad x + 1$

$= \quad x^4 + + + x +$

$x^4 + + + x + 1$

$= \quad + + + + 1$

T.e. [1 1 0 1 0 0] mod [1 0 0 1 1] = [0 0 0 1]

Проверяем [1 0 0 1 1] X [0 0 1 1] ⊕ [0 0 0 1]

= [1 1 0 1 0 1] ⊕ [0 0 1 1] = [1 1 0 1 0 0]

Sout[0][0] = Sin[0][0] ⊕ [0 0 0 1]

Sout[0][0] = [0 1 1 0] ⊕ [0 0 0 1] = [0 1 1 1]

ЛИТЕРАТУРА

Нечаев В.И. Элементы криптографии (Основы теории защиты информации).- Учеб. пособие. – М.:, ВШ., 1999.- 109 с.

Введение в криптографию. **Под общ. ред. В.В.Ященко.** – 4-е изд., доп. М.: МЦНМО, 2012 – 348 с. ISBN 978-5-4439-0026-1

ЛИТЕРАТУРА

Венбо Мао. Современная криптография: теория и практика.—М.: Издательский дом «Вильямс», 2005.—768 с.: ил. ISSN 5-8459-0847-7 (рус.)

Шнайер Б. Прикладная криптография. Протоколы, алгоритмы и исходный код на Си. – Москва: Вильямс, 2016. 1024 с.

ЛИТЕРАТУРА

Francisco Rodriguez-Henriquez, N.A. Saqib, A. Diaz-Perez, Cetin Kaya Koc.

Cryptographic Algorithms on Reconfigurable Hardware. - Springer, 2006.

A. Menezes, P. van Oorschot, S. Vanstone.

Handbook of Applied Cryptography.- CRC Press, 1996.

END # 12