Поточные шифры

Особенности.

1.Операции зашифрования и расшифр. вып-ся поразрядно.

2.Каждый символ шифртекста получается в рез-те поразрядной операции слож.по модулю два символа откр.текста и символа ключа

3.Поточный шифратор и деш-р требует задания *начального значения ключа*

4.Пот.шифры исп-ся в специальных приложениях и редко обсуждаются

Важнейшее достоинство ПШ перед блочными - высокая скорость шифрования - обеспечивается шифрование практически в реальном масштабе времени

Классический ПШ – **Шифр Вернама** (*One-time pad* — **схема одноразовых блокнотов,** 1917 г):

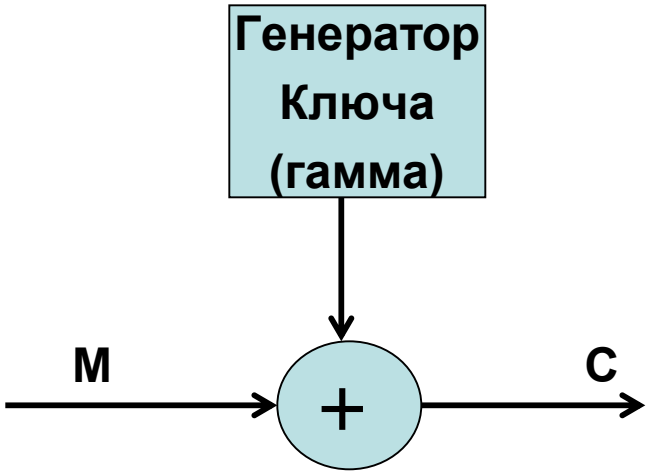
Зашифрование - открытый текст объединяется операцией «XOR» с ключом (одноразовым блокнотом или шифроблокнотом).

Ключ (**гамма**) должен обладать тремя критически важными свойствами:

- быть истинно случайным (последовательность, полученная с использованием любого алгоритма, является не истинно случайной, а псевдослучайной);
- совпадать по размеру с заданным открытым текстом;
- применяться только один раз.

В 1949 году К. Шеннон доказал абсолютную стойкость шифра Вернама - шифр Вернама является самой безопасной криптосистемой из всех возможных.

Идея гаммирования для ПШ



Генератор гаммы выдаёт ключевой поток (гамму): K=$k_1, k_2, k_3, \ldots, k_L$

Поток битов открытого текста:

M = $m_1, m_2, m_3, \ldots, m_L$.

Поток битов шифротекста : $c_i = m_i \oplus k_i$

Расшифрование производится операцией XOR между той же самой гаммой и зашифрованным текстом: $m_i = c_i \oplus k_i$

Если последовательность битов гаммы не имеет периода и выбирается случайно, то **взломать шифр невозможно.**

Типы поточных шифров:

1. Синхронные –

- поток гаммы генерируется независимо от открытого текста и шифротекста;
- для успешного расшиф-я необходимо синхрон-ть ключ с шифротекстом;

Свойства:

1. Искажение одного символа в шифротексте искажает только один символ в расшифр-м тексте (**+**),
2. Защита от любых вставок и удалений шифротекста, так как они приведут к потере синхронизации и будут обнаружены (**+**)
3. Нарушение синхр-ии (добавление или удаление символа) приводит к искажению всех сим-в после потери синхр-ии (**-**)

2. **Самосинхронизирующиеся** (***асинхронные***) (1946 г) –

- значение ключа зависит либо от исх текста, либо от шифротекста;
- поток ключей создается функцией ключа и фиксированного числа знаков шифртекста (**N):** внутреннее состояние генератора является функцией предыдущих **N** битов шифртекста - генератор потока ключей (при расшифровании) , приняв **N** битов, автоматически синхронизируется с шифрующим генератором

Свойства:

- Так как каждый знак открытого текста влияет на следующий шифртекст, статистические свойства открытого текста распространяются на весь шифртекст (**+**),
- ошибочно удаленный или добавленный символ (бит) вызывает только ограниченное кол-во ошибочных символов в дешифрованном тексте, после чего правильный текст восстанавливается (**+**)
- каждому неправильному биту шифртекста соответствуют **N** ошибок в открытом тексте) (**-**)

Генератор ключа (ГК)

Эффективный ГК – главная проблема ПШ: генерирование длинных ПСП

Наиболее частый алгоритм – на основе линейного конгруэнтного генератора; описыв-ся рекуррентным соотн-м:

$$x_{t+1} = (a*x_t + c) \bmod N,$$

x_0 – начальное значение ПСП, **a** – множитель, **c** – приращение, **N** - мощность алфавита

При **c=0** – мультипликативный конгруэнтный ген-р ПСП

Примеры параметров для PC с 32-разрядной архитектурой:

N= 2^{31} -1 = 2 147 483 647, a=16807; 630360016; 1078318381 4 1203248318; 397204094

Часто исп-е ГПСП:

$$x_{t+1} = (1176*x_t + 1476*x_{t-1} + 1776*x_{t-2}) \bmod 2^{32} - 5,$$

$$x_{t+1} = (2^{13} (x_t + x_{t-1} + x_{t-2}) \bmod 2^{32} - 5,$$

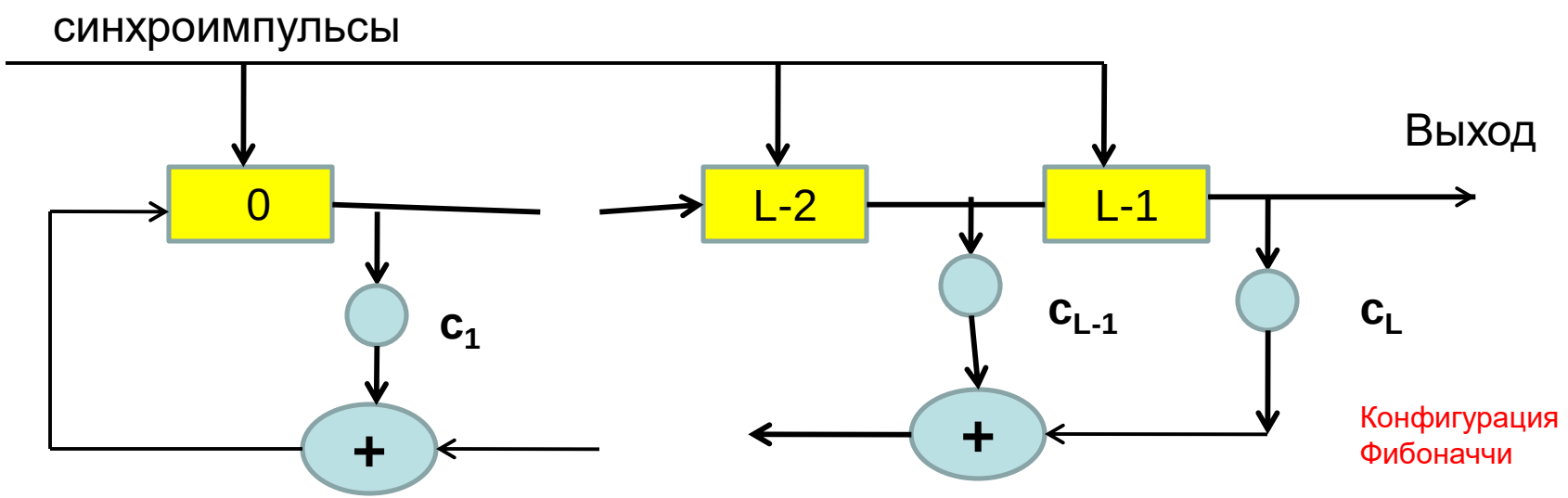
$$x_{t+1} = (1995*x_t + 1998*x_{t-1} + 2001*x_{t-2}) \bmod 2^{32} - 849,$$

$$x_{t+1} = (2^{19} (x_t + x_{t-1} + x_{t-2}) \bmod 2^{32} - 1629$$

Генераторы ПСП на основе регистров сдвига

РС – важнейший структурный компонент ЭЦВМ

РС состоит из триггеров и из функций обратных связей (ФОС)



Выходная послед-ть определяется начальным состоянием каждого Тг (общее число – **L**: от **0** до **L-1**) и видом ФОС,

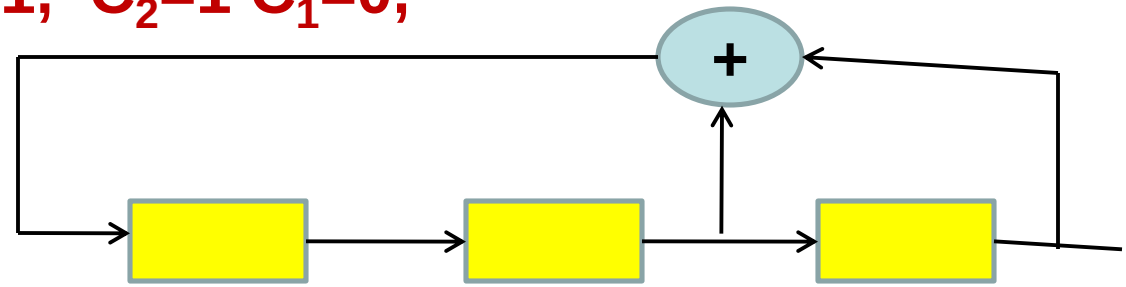
Чаще всего ФОС – XOR – РСЛОС (регистр сдвига с линейной обратной связью),

Период регистра сдвига — длина получаемой последовательности до начала её повторения

Пример. $C(x) = 1+c_2x^2 + c_3x^3 = x^3 + x^2 + 1 \rightarrow$ **320**

$C_3=1,\ C_2=1\ C_1=0,$

L=3



Конфигурация Фибоначчи

Многочлены $x^3 + x + 1$ (310)

и **$x^3 + x^2 + 1$ (320) является неприводимыми.**

Примеры других неприводимых многочленов:

210 $\rightarrow$ $c_2x^2 + c_1x + 1$

310, 410, 520, ….., 84320, …

Определение периода ПСП

Обратная связь	Разряды	регистра	сдвига	
1	0	0	1	1
0	1	0	0	2
1	0	1	0	3
1	1	0	1	4
1	1	1	0	5
0	1	1	1	6
0	0	1	1	7
1	0	0	1	

На выходе генератора буде последовательность: **1001011100101110010 11** …

Период равен $7 = 2^L - 1$

Свойства:

1.В течение каждой единицы времени (за такт)выполняются следующие операции:

содержимое ячейки **L-1** формирует часть выходной последовательности;

содержимое **i**-й ячейки перемещается в ячейку **i+1**

новое содержимое ячейки 0 определяется битом обратной связи, который вычисляется сложением по модулю с определёнными коэффициентами $\mathbf{c_i}$ битов ячеек .

2. Так как существует $\mathbf{2^L-1}$ разных ненулевых состояний регистра, то период последовательности, генерируемой РСЛОС при любом ненулевом начальном состоянии, не превышает $\mathbf{2^L-1}$.

3. Свойства ПСП зависят от **ассоциированного многочлена** :

$$\mathbf{C(x) = 1+c_1x+c_2x^2+ \ldots + c_Lx^L}$$

Его ненулевые коэффициенты называются **отводами**, (как и соответствующие ячейки регистра, составляющие значения аргументов функции обратной связи).

•Важное свойство многочлена **C(x)** - приводимость.

•Многочлен называется *приводимым*, если он может быть представлен как произведение двух многочленов меньших степеней с коэффициентами из данного поля (в нашем случае с двоичными коэффициентами).

Если нет, то многочлен называется *неприводимым*.

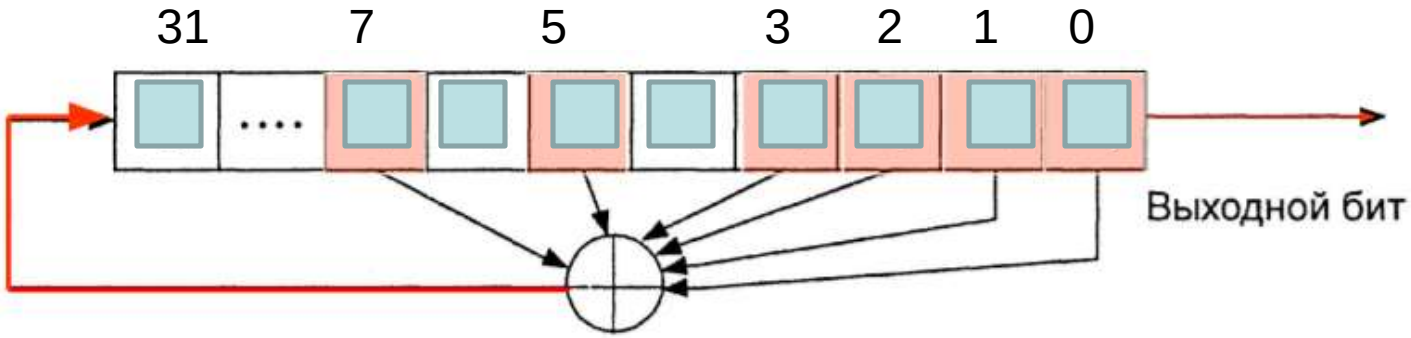
•Если многочлен является неприводимым, то период ПСП будет максимально возможным : $2^L - 1$

Пусть задан полином **32 7 5 3 2 1 0**:

$$x^{32} + x^7 + x^5 + x^3 + x^2 + x + 1$$

Все степени, за исключением старшей, задают последовательность отводов, отсчитываемую от правого (младшего) края регистра сдвига.
Член **x** (32) обозначает вход, который подается на левый (старший) разряд регистра.

Запись (32, 7, 5, 3, 2, 1, 0) означает, что для данного 32-битового регистра сдвига новый бит генерируется с помощью операции XOR над седьмым, пятым, третьим, вторым, первым и нулевом битами.



конфигурация Галуа

L	ПОЛИНОМ
1	$x+1$
2	x^2+x+1
3	x^3+x+1
	x^3+x^2+1
4	x^4+x+1
	x^4+x^2+1
5	x^5+x^2+1
	x^5+x^3+1
	$x^5+x^3+x^2+x+1$
	$x^5+x^4+x^2+x+1$
	$x^5+x^4+x^3+x+1$
	$x^5+x^4+x^3+x^2+1$
6	x^6+x+1
	x^6+x^3+1
	x^6+x^5+1
	$x^6+x^4+x^2+x+1$
	$x^6+x^4+x^3+x+1$
	$x^6+x^5+x^2+x+1$
	$x^6+x^5+x^3+x^2+1$
	$x^6+x^5+x^4+x+1$

L	ПОЛИНОМ
7	x^7+x+1
	x^7+x^3+1
	$x^7+x^3+x^2+x+1$
	x^7+x^4+1
	$x^7+x^4+x^3+x^2+1$
	$x^7+x^5+x^2+x+1$
	$x^7+x^3+x^3+x+1$
	$x^7+x^5+x^4+x^3+1$
	$x^7+x^5+x^4+x^3+x^2+x+1$
	x^7+x^6+1
	$x^7+x^6+x^3+x+1$
	$x^7+x^6+x^4+x+1$
	$x^7+x^6+x^4+x^2+1$
	$x^7+x^6+x^5+x^2+1$
	$x^7+x^6+x^5+x^3+x^2+1$
	$x^7+x^6+x^5+x^4+1$
	$x^7+x^6+x^5+x^4+x^2+x+1$
	$x^7+x^6+x^5+x^4+x^3+x^2+1$

L	полином	d_{min}
8	$x^8 + x^7 + x^6 + x^4 + 1$	
10	$x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1$	
5	$x^5 + x^2 + 1$	
10	$x^{10} + x^9 + x^8 + x^6 + x^5 + x^3 + 1$	
15	$x^{15} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^5 + x^3 + x^2 + x + 1$	
20	$x^{20} + x^{18} + x^{17} + x^{13} + x^{10} + x^9 + x^7 + x^6 + x^4 + x^2 + 1$	
25	$x^{25} + x^{24} + x^{21} + x^{19} + x^{18} + x^{16} + x^{15} + x^{14} + x^{13} + x^{11} + x^9 + x^5 + x^2 + x + 1$	
6	$x^6 + x + 1$	
12	$x^{12} + x^{10} + x^8 + x^5 + x^4 + x^3 + 1$	
18	$x^{18} + x^{17} + x^{16} + x^{15} + x^9 + x^7 + x^6 + x^3 + x^2 + x + 1$	
24	$x^{24} + x^{23} + x^{22} + x^{20} + x^{19} + x^{17} + x^{16} + x^{13} + x^{10} + x^9 + x^8 + x^6 + x^5 + x^4 + x^2 + x + 1$	

Задание 1. Записать выходную последовательность для генератора ПСП из предыд примера, если его начальное состояние будет:

а) 000,

б) 111

Задание 2. Построить генератор ПСП, заданный неприводимым многочленом 310. Записать выходную последовательность для генератора ПСП, если его начальное состояние будет:

а) 010,

б) 101.

Определить период.

Задание 3. Построить генератор ПСП, заданный многочленом 3210. Определить период.