**Потоковый шифр** – симм. шифр, преобр. каждый символ mi откр. текста в символ зашифрованного ci, зависящий от ключа и расположения символа в тексте.

**2 класса:** *синхронные* и *асинхр*.

**Гамма** – посл-сть для зашифрования,   
т.е. *выходная гамма* – ключевой поток (ключ) для сообщения

**Синхр. ПШ (СПШ)** – поток ключей генер. независимо от откр. текста и шифротекста.  
\* Ошибок нет, пока шифр. и дешифр работают синхронно : для этого м. разбить М на отрезки, начало и конец выделить спец.маркером (стр.79)  
\* Уязвимы к атакам на осн. изменения отд. бит шифротекста

**Самосинхронизирующиеся ПШ** – символы ключ.гаммы зависят от исх. секретного ключа шифра и от последних знаков C.  
\* генератор потока ключей – ф-я неск. предыдущих битов C => он авто- синхроиз с генератором гаммы  
\* искаж 1 бит ci == искаж неск битов гаммы (и расшифр сообщ)

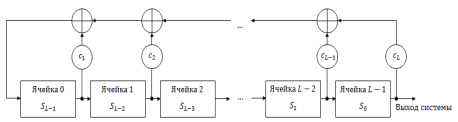
**Генераторы ключевой инфы:**

Генераторы вырабатывают (псевдо-)случайные ключ.посл-сти (ПСП)  
\* **случ. числа** – посл-сть элем, каждый из кот. не мб предсказан на основе предшест. элементов  
\* **псевдослуч.** – посл-сть элем, полученная в рез. вып-я нек. алгоритма

**Линейный конгруэнтный генератор:**

опис. соотн: xt+1 = (a \* xt + c) mod n  
 x.. – члены числ. посл-сти  
 а, с, n – константы  
 период не выше n  
генератор порождает случ. числа с макс. периодом =с  
обычно с устан 2B-1 или 2B , b – длина слова [б]  
+ просты, выс. скорость  
+ исп. в моделировании и матем. статистике  
- не рек в криптографии, т.к. легко восст посл-сть

**Генератор ПСП на основе регистров сдвига (РС):**

+ легко реализ на основе цифр. логики  
**РС с лин. обр. связью (РСЛОС)** сост из 2 частей:  
 \* регистры сдвига  
 \* ф-я обр. связи (на осн. XOR)  
РСЛОС строй на осн. примитивных породающих многочленов 

**Генератор ПСП на основе алгоритма RSA:**

опис. соотн: xt = (xt-1)e mod n  
 n,p,q – нач. параметры (n=p\*q)  
 e – взаимно простое число с (p-1)\*(q-1)  
 xo – нек. случайное нач. значение  
безопасность опир. на сложность RSA, т.е. на разложении n на простые сомнож

**Генератор ПСП на основе алгоритма BBS:**

на основе квадратичных вычетов, медленный  
опис. соотн: xo = x2 mod n  
 n=p\*q (при делении p,q на 4 дб остаток 3)  
 х – *число Блюма* (вз-простое с n)  
 xt = (xt-1)2 mod n  
 xt = (xo)a mod n, где а=2t mod ((p-1)(q-1))

Пр: p=11, q=19  
 11mod 4=3, 19mod 4=3  
 n=pq = 11\*19 = 209  
 выберем х взаимно простое с n (например 3)  
 xo = 32 mod 209 = 9  
 x1 = 92 mod 209 = 81  
 x2 = 812 mod 209 = 82 …

**Потоковый шифр RC4:**

\* ПШ с переменным размером ключа, гамма не завис от откр.текста  
\* строится на осн. генератора ПСП, на его вход запис ключ [40-2048]  
\* ядро алг – ф-я генерации ключ. потока  
\* др. часть алг – ф-я инициализации – исп. ключ перем.длины Ki для создания нач. сост. генератора ключ. потока  
\* в основе алг – размер блока n   
\* внут. состояние шифра опр-ся массивом слов S размером 2n  
\* генератор ключ. потока перест. значения в S и к.раз выбир. одно в кач-ве рез.  
\* *один цикл*: опред. одно слово [n] K из ключ.потока, кот. потом суммир с C



Пусть наш ключ k={1, 2, 3, 4, 5, 6}  
1) Заполняем линейно S [16]: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15  
2) Заполняем K, записывая ключ неск. раз: 1 2 3 4 5 6 1 2 3 4 5 6 1 2 3 4  
3) Перемешаем S по алг? 10 13 14 12 2 15 6 4 5 3 1 9 8 7 0 11  
4) Генерируем ПСП (n=8 – числа ПСП будут иметь 8 бита)

………………………..

**ЗАДАНИЕ: (стр.91)**

1) генерация ПСП – BBS (вар. 3)  
 парам: n=256, p,q – обосновать выбор по соглас. с преподом

2) RC4 + оценка скорости генерации ПСП  
 n=8, ключ = {1, 11, 21, 31, 41, 51}

1. В чем состоит особенность потоковых шифров?

шифруют 1 символ в завис от ключа и положения в тексте (примен xor к тексту)  
шифруют информацию по одному биту за такт шифрования.

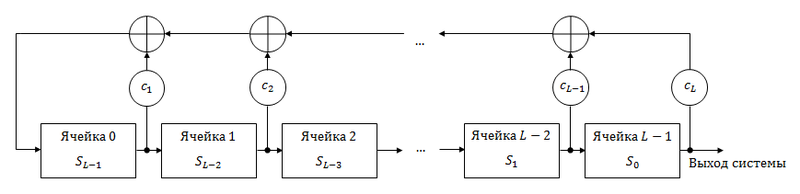
2. В чем состоят преимущества и недостатки синхронных и асинхронных потоковых шифров?

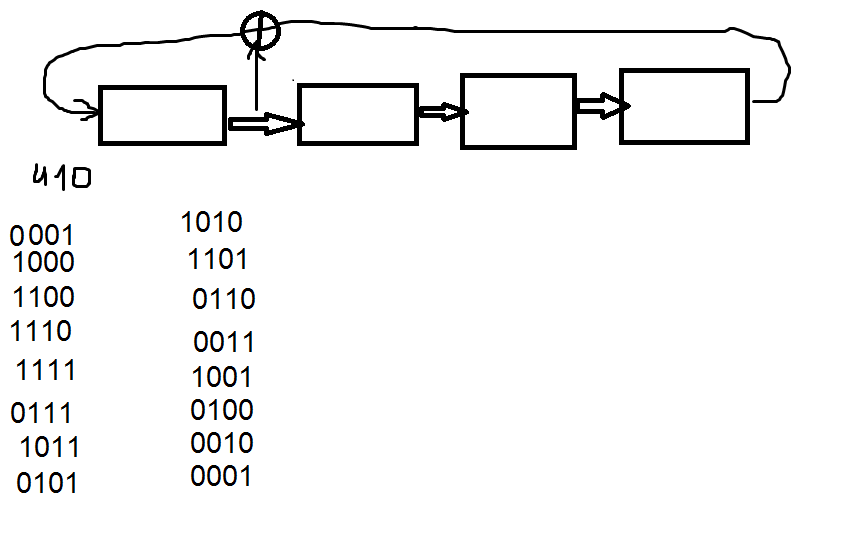
3. Какими свойствами должен обладать генератор псевдослучайных чисел для использования в криптографических целях?

4. Дать характеристику линейным конгруэнтным генераторам. Области их применения.

5. Значения x0, x1, x2, x3, полученные с помощью линейного конгруэнтного генератора, равны соответственно: 1, 12, 3, 6. Найти параметры а, с и n генератора ПСЧ, удовлетворяющие (6.1).

6. Представить общую структурную схему генератора ПСП на основе регистров сдвига с линейной обратной связью. Пояснить особенности его функционирования.





Если многочлен является неприводимым, то период ПСП при ненулевом начальном условии (ненулевом состоянии) регистра будет максимально возможным: 2L – 1.

7. Синтезировать структурную схему генератора ПСП на основе регистров сдвига с линейной обратной связью, формально обозначаемого следующим образом: а) 3210, б) 420, в) 5410, г) 520, д) 84320. Составить таблицу состояний генератора и определить период ПСП.

8. Определить первые 12 бит ПСП, задаваемого формально в виде чисел 5410, если начальные состояния ячеек (слева-направо) соответствуют последовательности 10101.

9. Как устроен генератор ПСП на основе RSA? На чем основана криптостойкость реализуемого алгоритма?

10.Вычислить х1, х5 , х9, х11 по методу генерации псевдослучайных чисел BBS, если p = 11, q = 19, х = 3.

11.Пояснить базовый алгоритм, реализованный в шифре RC4.

12. Пояснить принципы формирования истинных случайных последовательностей, основанных на «естественных случайностях».