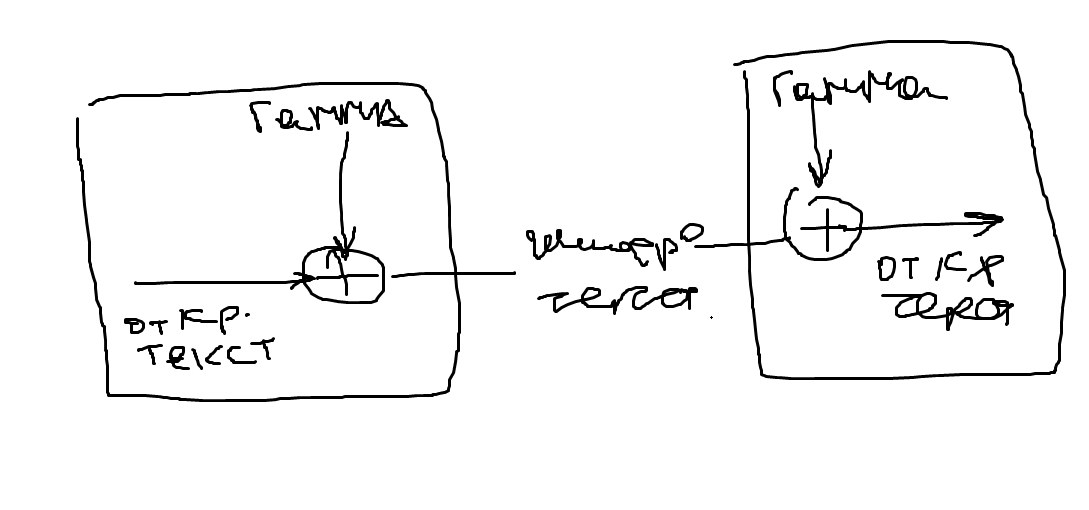
**Потоковые** – симметричный. каждый символ (одна буква, бит и реже байт) открытого текста шифруется в отедльный символ закрытого с помощью ключа и расположения в тексте.

Делятся на **синхронные** (гамма генерируется независимо от открытого и шифротекста. Поэтому она избавлена от распространения ошибок. Работают корректно до тех пор, пока устройства шифрования и дешифрования работают синхронно. Для борьбы с расинхронизации Обычно большие блоки разбиваются на маленькие и вставляются туда контрольные суммы для обеспечения синхронизации) и **асинхронные** (зависит от исходного секретного ключа и конечного числа последних битов зашифрованного сообщения. Простыми словами она зависит от битов которые уже были зашифрованы и если принимющая сторорна получит нужное количество битов, то остаьлные могут затеряться и процесс все равно будет продолжаться).

Основная **задача** потоковых шифров – сформировать гамму – последовательность для зашифрования (выходная гамма это ключ для сообщения).

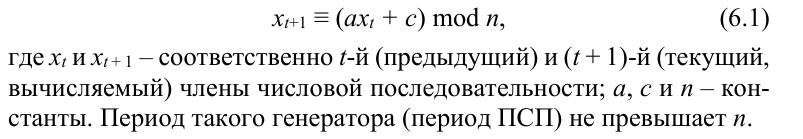


**Схема потокового шифра**

**Ключевые последовательности** – СП (случ. Посл.) и ПСП (псевдо случайные последовательности) – вырабатываются блоками систем потокового шифрования – генераторами.

**Линейный конгруэнтный генератор** – генератор ПСП

Икс т + 1 тройное равно (ах+с)модн

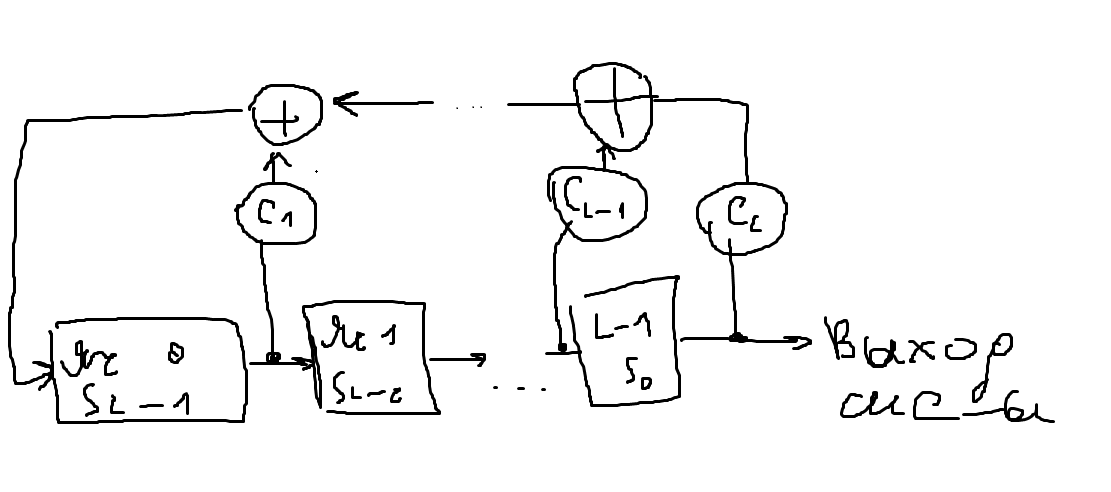


Достоинства: простота и быстрое получение ПСП

Недостатки: низкая криптостойкость

**Генератор ПСП на основе регистров сдвига**

Регистр сдвига с линейной обратной связью **РСЛОС** состоит из двух частей: РС и функция обратной связи (сумматоры XOR – плюсик сверху блок-схемы).



**Общая схема РСЛОС**

Он строится на основе примитивных полиномов. Если он не приводим, значит период ПСП макс – 2L-1

**Генератор ПСП на основе алогоритма RSA**

Сроится на основе

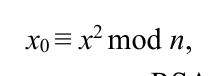


Сначача подбираются взаимно простые p и q, n = p \* q, функция эйлера f = (p - 1)(q - 1), 1 < e < f

Безопасность определяется сложностью разложения n на простые множители.

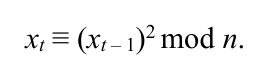
Выходом генератора на t-шаге является младший бит числа xt.

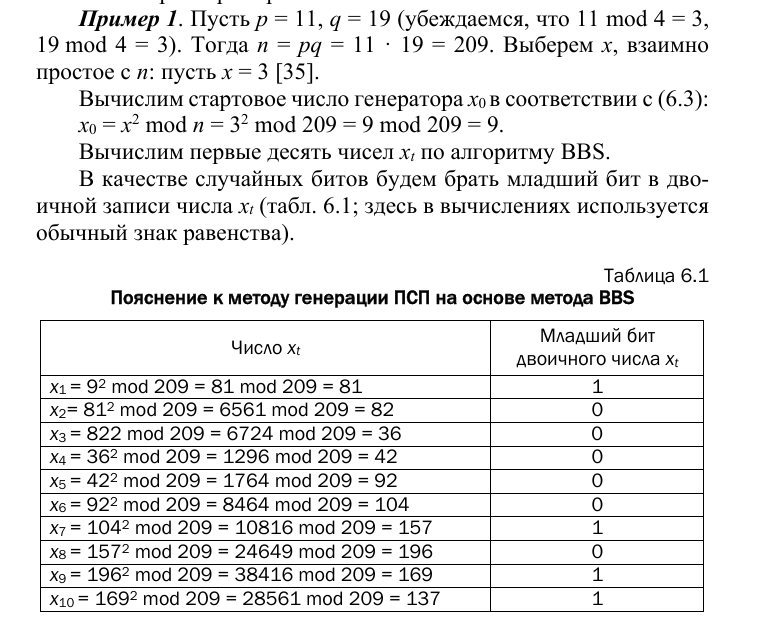
**Генератор ПСП на основе BBS**



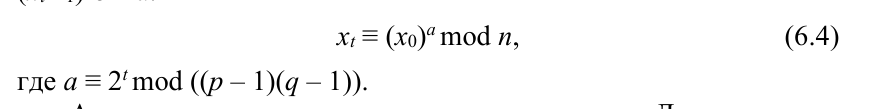
n=p\*q, p и q – простые числа. p(q)mod4=3. Число x – взаимно простое с n.

Выходом генератора на t-м шаге является младший бит числа xt:





Безопасность хромает при известных p и q, ведь можно найти значение xt не зная xt-1 по следующего выражению



**Потоковый шифр RC4 (переменный размер ключа. Гамма не зависит от открытого текста)**

