Кафедра информационной безопасности

Раздел №2: «Основные классы шифрсистем»

Тема №1: «Шифрсистемы с секретным ключом»

Контроль усвоения учебного материала предыдущих занятий

1
Вариант

1. Дайте определение понятию «блочная шифрсистема».
2. Охарактеризуйте синхронные поточные шифрсистемы и перечислите их особенности в отношении ошибок синхронизации.
3. Перечислите требования к шифрующему блоку поточных шифрсистем.

2
Вариант

1. Дайте определение понятию «поточная шифрсистема».
2. Охарактеризуйте поточные шифрсистемы с самосинхронизацией и перечислите их особенности в отношении ошибок синхронизации.
3. Перечислите требования к управляющему блоку поточных шифрсистем.

Занятие №2

«Построение поточных шифрсистем»

Учебные и воспитательные цели:

1. Изучить принципы построения поточных шифрсистем.

2. Раскрыть вопросы синхронизации в поточных шифрсистемах.

3. Рассмотреть параметры, определяющие надежность поточной шифрсистемы.

4. Активизировать на изучение вопросов обеспечения безопасности информации криптографическими методами.

Учебные вопросы:

1. Типовые генераторы ключевого потока

2. Пример реальной поточной шифрсистемы

3. Методы анализа поточных шифрсистем

Первый учебный вопрос:

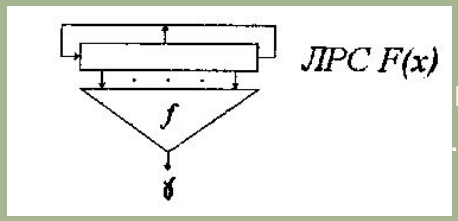
«Типовые генераторы ключевого потока»

Способы усложнения аналитического строения линейных рекуррент

Фильтрующие генераторы

Первый способ заключается в применении к элементам линейной рекуррентной последовательности некоторой функции *f*.

"Фильтрующая" функция *f* должна выбираться так, чтобы выходная последовательность имела распределение, близкое к равномерному распределению, и высокую линейную сложность.



ктеристический многочлен, определяющий закон рекурсии

Рис. 1. Фильтрующий генератор

Комбинирующие генераторы

Второе направление синтеза псевдослучайных последовательностей с высокой линейной сложностью связано с использованием в одной схеме нескольких линейных регистров сдвига. Генератор псевдослучайных последовательностей, реализующий усложнение нескольких линейных рекуррент с помощью одной общей функции усложнения, получил название комбинирующего генератора (рис. 2).

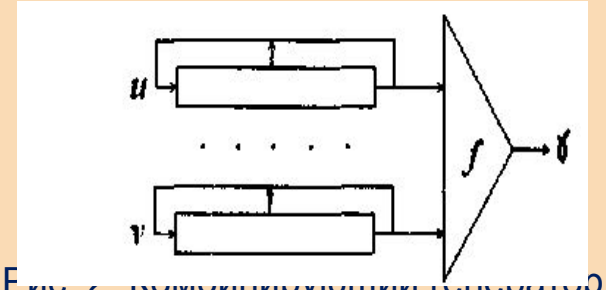


Рис. 2. Комбинирующий генератор

Способы усложнения аналитического строения линейных рекуррент

Композиции линейных регистров сдвига

Рассмотрим еще один тип генераторов, представляющий собой композицию линейных регистров сдвига. Так называется схема, в которой выход одного из регистров подается на вход другого регистра (рис. 3).

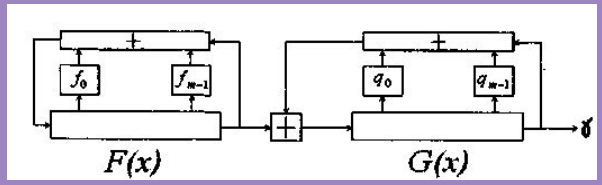


Рис. 3. Композиция регистров

Схемы с динамическим изменением закона рекурсии

Альтернативный способ усложнения ЛРП состоит в изменении закона рекурсии в процессе работы криптографического алгоритма. Привлекательным представляется использование нелинейной логики в цепи обратной связи регистровых преобразований. Однако общая теория подобных схем еще недостаточно разработана, в связи с чем трудно гарантировать необходимые свойства соответствующих последовательностей.

Один из путей построения подобных схем основан на динамическом изменении закона рекурсии линейного регистра сдвига.

Схемы с элементами памяти

Один из наиболее широко известных классов датчиков псевдослучайных чисел, построенных с использованием памяти, составляют генераторы Макларена—Марсальи.

Пусть имеются три последовательности и массив памяти. Первая последовательность определяет, какие знаки заносятся в память, вторая последовательность управляет процессом записи этих элементов в память, а третья — процессом считывания из памяти элементов выходной последовательности.

Последовательность ***v*** определяет адреса, по которым в память записываются элементы последовательности ***u***.

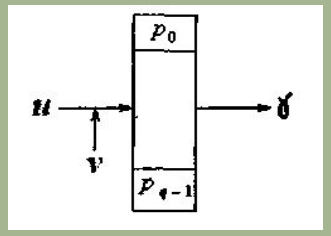


Рис. 4. Генераторы с памятью

Второй учебный вопрос:

«Примеры поточных шифрсистем»

2.1. ШИФРСИСТЕМА A5

A5 — шифрсистема гаммирования, применяемая для шифрования телефонных сеансов в европейской системе мобильной цифровой связи GSM (Group Special Mobile). В открытой печати криптосхема A5 официально не публиковалась. Британская телефонная компания передала всю техническую документацию Брэдфордскому университету. Через некоторое время детали о конструкции A5 стали просачиваться в печать и, в конце концов, появились в INTERNET.

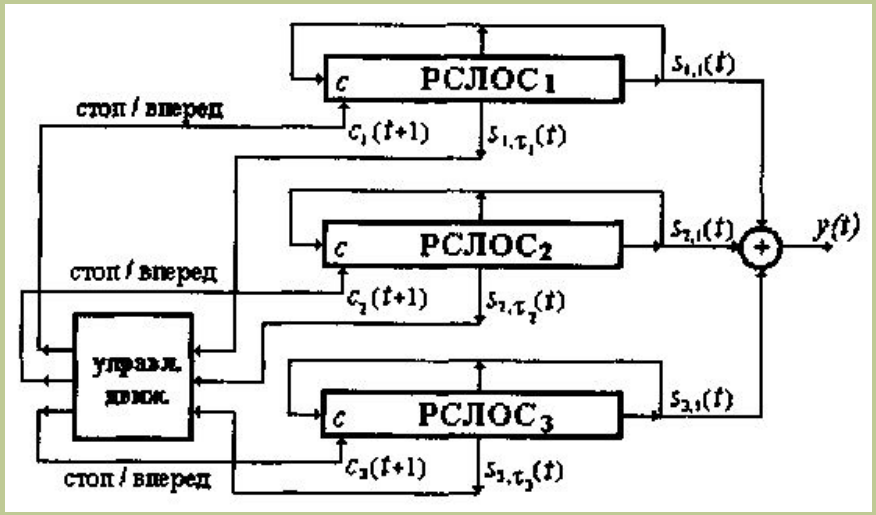


Рис. 5. Криптосхема A5

В системах GSM алгоритм A5 используется для защиты информации между абонентом и базовой станцией, так что фактически в сеансе связи двух абонентов шифрование происходит дважды. Это дает возможность использования атаки на основе известного открытого текста.

2.2. ШИФРСИСТЕМА Гиффорда

Д. Гиффорд предложил схему поточного шифра, которая использовалась с 1984 по 1988 г. агентством Associated Press. Криптосхема генератора (см. рис. 6) представляет собой 8-байтовый регистр сдвига с линейной функцией обратной связи ***f*** и нелинейной функцией выхода ***h***. Ключом являются 64 бита начального заполнения регистра. Схема реализует шифр гаммирования.

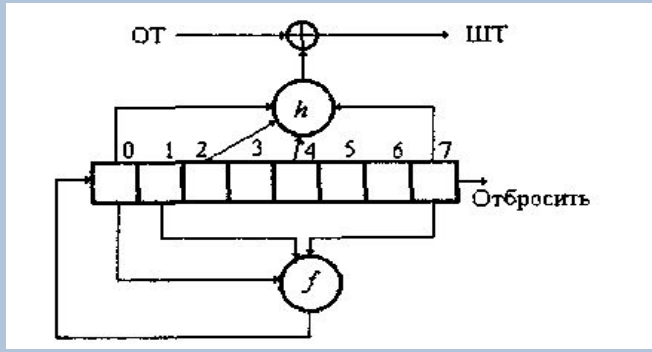


Рис. 6. Шифрсистема Гиффорда

2.3. АЛГОРИТМ RC4

RC4 представляет собой потоковый шифр с переменной длиной ключа, разработанный в 1987 г. Роном Ривестом для компании RSA Data Security, Inc. В течение 7 лет этот шифр лицензировался компанией только на условиях неразглашения. Однако в 1994 г. он был анонимно опубликован в Интернете и с тех пор стал доступен для независимого анализа.

Алгоритм работает в режиме **OFB** (***Output Feed Back*** **- режим обратной связи по выходу**). Ключевая последовательность не зависит от исходного текста.

Шифрование по этому алгоритму примерно в 10 раз быстрее, чем шифрование DES при программной реализации.

Третий учебный вопрос:

«Методы анализа поточных шифрсистем»

Методы криптоанализа на примере поточных шифров гаммирования

Подходы:

1). В первую очередь необходимо исследовать *вероятностные характеристики гаммы*. Как мы уже знаем, имеются подходы к получению оценок вероятностей элементов неравновероятной гаммы по шифртексту, которые можно использовать при бесключевом чтении.

2). Второй подход связан с попытками *линеаризации* уравнений гаммообразования, то есть сведения задачи нахождения ключей криптографических алгоритмов к решению некоторой системы линейных уравнений. При таком подходе определяющую роль играет линейная сложность исследуемых последовательностей. Значение линейной сложности определяет размеры системы линейных уравнений, которую надо решить для определения ключа по известной шифрующей гамме.

3). К вопросу о статистических зависимостях в шифрующей гамме примыкают методы анализа, основанные на наличии у функции усложнения хороших *приближений в классе линейных функций*. Примером отображений, не имеющих линейных статистических аналогов хорошего качества, является класс бент-функций. В случае наличия у функции усложнения линейного приближения криптоаналитик может заменить исследуемую схему схемой с линейной функцией усложнения.

[!] При оценке криптографических качеств поточных шифров, помимо алгебраических и статистических свойств шифрующей гаммы, необходимо учитывать также наличие между знаками гаммы зависимостей комбинаторного характера.

Вывод: При создании криптографически стойких поточных шифрсистем необходимо учитывать возможности применения криптоаналитиком всей совокупности статистических, аналитических и комбинаторных свойств используемых преобразований. Вывод о криптографической стойкости конкретного шифра может быть сделан только на основе его комплексных исследований, проведенных с привлечением квалифицированных специалистов-криптографов.