

Министерство образования и науки Российской Федерации
Ярославский государственный университет им. П. Г. Демидова
Кафедра компьютерных сетей

Математические методы защиты информации

Часть 2

Методические указания

Рекомендовано
Научно-методическим советом университета для студентов,
обучающихся по специальности
Прикладная математика и информатика

Ярославль 2011

УДК 51(075)
ББК В 13я73
М 33

*Рекомендовано
Редакционно-издательским советом университета
в качестве учебного издания. План 2010/2011 учебного года*

Рецензент: кафедра компьютерных сетей
Ярославского государственного университета им. П. Г. Демидова

Составитель М. В. Краснов

Математические методы защиты информации. Ч. 2 : методические
М 33 указания / сост. М. В. Краснов; Яросл. гос. ун-т им. П. Г. Демидова. –
Ярославль : ЯрГУ, 2011. – 44 с.

Основное использование вычислительной техники связано с хранением информации. Естественно, возникает задача защиты информации от несанкционированного использования. В работе сформулированы основные идеи создания блочных симметричных алгоритмов. Наиболее известные из них подробно описаны. Рассмотрена проблема управления ключами, которая возникает при работе с симметричными шрифтами.

Предназначены для студентов, обучающихся по специальности 010501.65 Прикладная математика и информатика (дисциплина «Математические методы защиты информации», блок ДС), очной формы обучения.

УДК 51(075)
ББК В 13я73

© Ярославский государственный
университет им. П. Г. Демидова, 2011

Учебное издание

Математические методы защиты информации

Часть 2

Методические указания

Составитель **Краснов** Михаил Владимирович

Редактор, корректор М. В. Никулина
Верстка Е. Л. Шелехова

Подписано в печать 23.06.2011. Формат 60×84 ¹/₁₆.
Бум. офсетная. Гарнитура "Times New Roman".
Усл. печ. л. 2,56. Уч.-изд. л. 2,03.
Тираж 50 экз. Заказ

Оригинал-макет подготовлен
в редакционно-издательском отделе Ярославского
государственного университета им. П. Г. Демидова.
Отпечатано на ризографе.

Ярославский государственный университет им. П. Г. Демидова.
150000, Ярославль, ул. Советская, 14.

Введение

В настоящее время использование электронной вычислительной техники в различных областях человеческой деятельности все более и более возрастает. Однако чаще всего вычислительная техника используется для хранения и передачи информации. Естественно, возникает задача защиты информации от несанкционированного использования. Среди способов защиты информации одним из наиболее распространенных методов является криптографический метод. Он предусматривает такое преобразование информации, при котором она становится доступной для прочтения лишь обладателю некоторого секретного параметра (ключа).

Опишем задачу защиты информации с помощью криптографического метода. Отправитель хочет послать получателю по каналу, который не является безопасным, текст T . Взломщик хочет перехватить передаваемую информацию. Отправителю нужно так преобразовать сообщение, чтобы взломщик не смог прочитать исходный текст T из перехваченного сообщения, а получатель мог бы за приемлемое время восстановить исходный текст из полученного сообщения.

Чтобы решить поставленную задачу, отправитель шифрует исходный текст T с помощью некоторого преобразования E_k , где k – ключ шифрования. Шифртекст $C = E_k(T)$ передается по каналу связи.

Получатель должен уметь расшифровать шифртекст – восстановить исходный текст T с помощью некоторого преобразования $D_{\tilde{k}}$, где \tilde{k} – ключ расшифрования: $T = D_{\tilde{k}}(C)$.

Если отправитель знает ключ k , то он может зашифровывать информацию; если получатель знает ключ \tilde{k} , то он может расшифровывать сообщение.

Перед взломщиком стоит более сложная задача: он должен найти ключ \tilde{k} или свой способ дешифровки.

Алгоритмы, используемые в современных криптосистемах, можно разделить на два типа: симметричные, в которых ключ расшифрования легко находится по ключу шифрования; с открытым ключом, в которых ключ расшифрования трудно найти даже при известном ключе шифрования.

С другой стороны, симметричные шифры можно разделить на два типа шифров: блочное и потоковое шифрование. Блочное шифрование – в этом случае исходное сообщение разбивается на блоки фиксированной размерности (например, 64 или 128 бит), которые потом и шифруются. Потоковое шифрование используется, когда нельзя разбить исходное сообщение на блоки. Например, каждый символ исходного сообщения должен быть зашифрован, не дожидаясь остальных данных.

В представленных методических указаниях основное внимание будет уделено симметричным блочным шифрам.

Можно сказать, что блочные шифры реализуются путем многократного применения к блокам открытого текста некоторых базовых преобразований. Обычно используются базовые преобразования двух типов – это локальные преобразования над отдельными частями шифруемых блоков и простые преобразования, переставляющие между собой части шифруемых блоков. Первое преобразование усложняет восстановление взаимосвязи статистических и аналитических свойств открытого и зашифрованного текстов, а второе преобразование распространяет влияние одного знака открытого текста на большое число знаков шифра.

Сформулируем основные конструкции, которые часто используются в процессе создания симметричного блочного шифра:

- сеть Фейстеля (рис. 1) предполагает разбиение рассматриваемого вектора на несколько подблоков (например, на два), один из блоков обрабатывается некоторой функцией f , а результат складывается по модулю два с одним или несколькими из оставшихся подблоков.

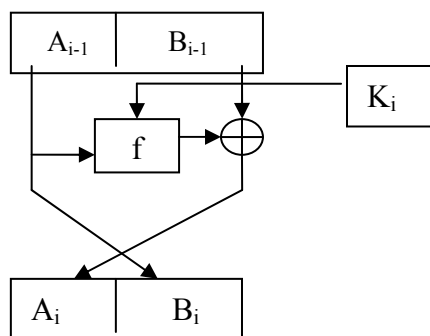


Рис. 1. Сеть Фейстеля

Легко заметить, что в качестве дополнительного параметра функции f является раундовый ключ K_i . Раундовый ключ получается из исходного ключа обычно путем развертывания.

- SP-сети (рис. 2). Обработка данных сводится в основном к заменам (например, с помощью таблицы замен) и перестановкам, которые зависят от ключа.

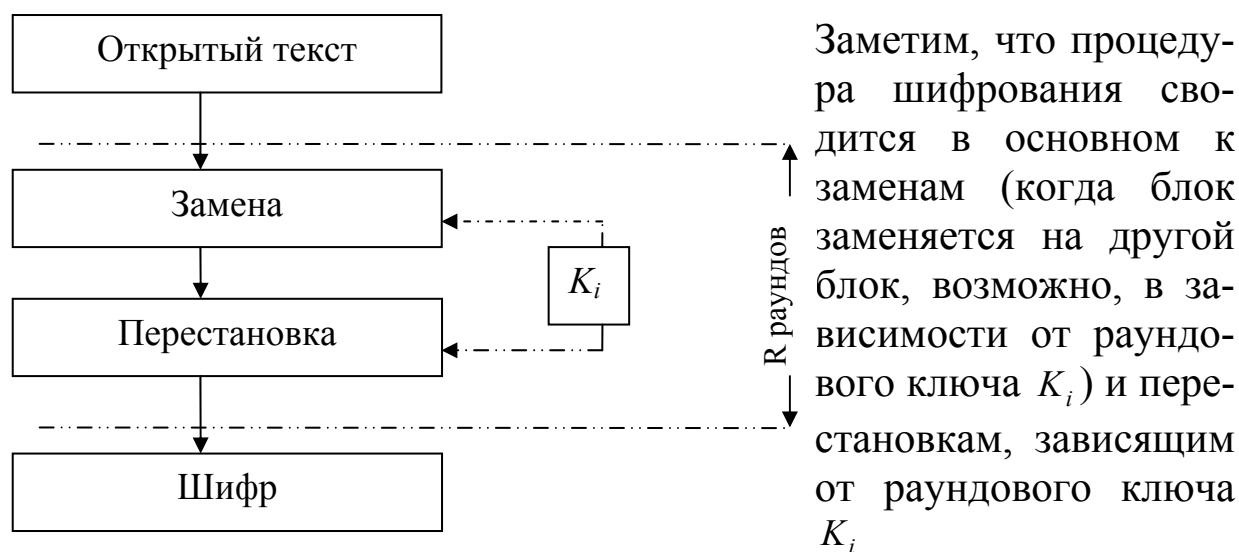


Рис. 2. SP-сеть

Самая простая сеть состоит из слоёв двух типов, используемых многократно по очереди. Первый тип слоя – Р-слой, состоящий из Р-блока большой разрядности, за ним идёт второй тип слоя – S-слой, представляющий собой большое количество S-блоков малой разрядности.

Также популярны алгоритмы, построенные на основе SP-сети со структурой «квадрат». В этом случае обрабатываемый в процессе работы алгоритма блок данных представляется в виде двумерного байтового массива. Криптографические преобразования могут выполняться как над отдельными байтами массива, так и над его строками или столбцами.

Режимы работы блочных шифров

Обычно при реальном применении используется не только сам алгоритм шифрования-дешифрования, но и специальные режимы работы блочных симметричных шифров. Наиболее популярны четыре режима: электронная шифрованная книга, сцепление шифрованных блоков, обратная связь по шифру, обратная связь по выходу¹. Этих режимов хватает, чтобы использовать

¹ Используются и другие режимы, например режим сцепления блоков вида: